ServerView Suite

iRMC S2 - integrated Remote Management Controller

2009 年 12 月版

目次

1 章 iRMC S2 の概要

最新のサーバシステムはますます複雑になり、システム管理面の必要条件も増加しています。

こうした状況に対応するため、システムを集中制御する BMC（Baseboard Management Controller：

ベースボード管理コントローラ）とインテリジェントなプラットフォーム管理ハードウェアの間に抽象化されたメッセージベースの標準インターフェースを実現しようと、多くのベンダーが提携して IPMI（Intelligent Platform Management Interface）イニシアティブが設立されました。IPMI の詳細については、「1.4 IMPI のテクニカルな背景」（→ P.18）を参照してください。

iRMC S2（**i**ntegrated **R**emote **M**anagement **C**ontroller：リモートマネジメントコントローラ）は、統合 LAN 接続および従来は RSB（RemoteView Service Board：リモートサービスボード）のようなプラグインボードを追加した場合にのみ利用可能だった拡張機能を実現する BMC です。これにより、システムの状態に関係なく PRIMERGY サーバの総合制御が可能です。特に「Out-bound」状態の PRIMERGY サーバに対して有効です。

図 1：PRIMERGY サーバのシステムボード上の iRMC S2

iRMC S2 は最新 PRIMERGY サーバのシステムボード上にある自立したシステムであり、専用のオペレーティングシステムおよび専用 Web サーバ、独立ユーザー管理、独立警告システムがあります。サーバがスタンバイモードの場合でも、iRMC S2 の電源は ON のままです。

本書では、iRMC S2 の設定方法および利用可能なさまざまなユーザーインターフェースを説明してい ます。

1.1 本書の目的と対象

本書は、システム管理者およびネットワーク管理者、ハードウェアおよびソフトウェアの十分な知識を持ったサービススタッフを対象としています。IPMI の背後の基本的なテクノロジーに関して説明を行った後、次の事項に関する詳細を説明します。

– iRMC S2 へのログオン
– iRMC S2 の設定
– iRMC S2 のユーザー管理
– iRMC S2 によるビデオリダイレクション
– iRMC S2 によるリモートストレージ
– iRMC S2 Web インターフェース
– iRMC S2 の Telnet/SSH ベースインターフェース（リモートマネージャ）
– サーバ設定による iRMC S2 の設定 – ファームウェアのアップデート
– iRMC S2 によるオペレーティングシステムのリモートインストール
– IPMI OEM コマンド

ServerView リモートマネジメント関連文書

ServerView リモートマネジメントおよび ServerView に関する詳細については、「関連情報」（→ P.495）を参照してください。

サービス

PRIMERGY サーバのリモートマネジメントに関する質問は、サービス＆サポートパートナーにお問い合わせください。

参照情報
http://www.ts.fujitsu.com

1.2 iRMC S2 のファンクション

iRMC S2 は広範囲にわたるファンクションを標準サポートしますが、AVR（Advanced Video Redirection：ビデオリダイレクション）およびリモートストレージと組み合わせれば、さらに 2 つの PRIMERGY サーバリモートマネジメント拡張ファンクションが利用可能です。AVR およびリモートストレージの使用には、別売のライセンスキーが必要です。

標準 **iRMC S2** ファンクション

- ブラウザアクセス

  iRMC S2 には専用 Web サーバがあるため、管理端末から標準 Web ブラウザでアクセスできます。

- セキュリティ（SSL、SSH）

  HTTPS／SSL によるセキュアな Web サーバアクセスおよびセキュアなグラフィカルコンソールリダイレクション（マウスおよびキーボード付き）をサポートします。iRMC S2 へのアクセスは、リモートマネージャから SSH による暗号化設定を行って接続を保護できます。リモートマネージャの iRMC S2 インターフェースは、英数字専用です。

- ServerView 統合

  ServerViewエージェントがiRMC S2を検出し、自動的に関連サーバに適用します。したがってServerView リモートマネジメントフロントエンドを使って、ServerView Operations Manager から iRMC S2 Web インターフェースおよびテキストコンソールリダイレクトを直接開始できます。

- 電源制御

  システムの状態に関係なく、次の 3 つの方法でリモート管理端末から管理対象サーバの電源の投入および切断が可能です。

  – iRMC S2 Web インターフェース

  – リモートマネージャおよび CLP（Command Line Interface：コマンドラインインターフェース）
  – スクリプト

- 消費電力制御

  iRMC S2 は、管理対象サーバの消費電力制御を総合的に行います。最小消費電力から最大パフォーマンスまで、電力制御モードを指定できます。モードは、必要に応じて切り替えられます。

- CSS（Customer Self Service：カスタマセルフサービス）

  変化したサーバコンポーネントが CSS コンポーネントの場合、iRMC S2 Web インターフェース上のサーバコンポーネントおよびセンサ、電源ユニットなどのためのサマリー表の各列に情報が表示されます。さらに、SEL（System Event Log：システムイベントログ）のエラーリストには、CSS コンポーネントが始動したあらゆるイベントが表示されます。

- テキストコンソールのリダイレクション

  ServerView リモートマネジメントフロントエンドから、iRMC S2 への Telnet/SSH セッションを開始できます。テキストコンソールのリダイレクションが開始され、リモートマネージャが起動します。iRMC S2 インターフェースは、英数字専用です。

- BMC の基本機能

  iRMC S2 は、電圧監視およびイベントログ、リカバリ制御などの BMC 基本機能をサポートしています。

- 「ヘッドレス」システム操作

  管理対象サーバに、マウスもしくはモニタ、キーボードは必要ありません。これにより、コストの 低減、筐体のケーブリングのより一層の簡略化およびセキュリティの強化を実現しています。

- 識別灯

  筐体ロッカー内に多数設置されている場合などにシステムが容易に識別できるように、iRMC S2 Web インターフェースから識別灯を起動できます。

- Error LED

  Error LED は、管理対象システムの状態と CSS の状態を常時示しています。

- 電源 LED

  電源 LED は、サーバの電源の ON ／ OFF の状態を示しています。

- LAN

  サーバ内蔵のシステム NIC（Network Interface Card）の LAN インターフェースには、管理 LAN 専用になっているシステムと設定を選べるシステムがあります。

  – 管理 LAN 専用に設定
  – 管理 LAN とシステムで共用するように設定
  – システム用に完全に開放

  レンチ記号がついたポートは、iRMC S2 用です。図 .7（→ P.33）を参照してください。

- CLP（Command Line Interface：コマンドラインインターフェース）

  リモートマネージャに加えて、iRMC S2 は DMTF（Distributed Management Task Force : 分散管理タスクフォース）標準の SMASH CLP（**S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol）をサポートしています。

- インタラクティブもしくはスクリプトベースでの容易な設定

  iRMC S2 は、次の方法で設定できます。

  – iRMC Web インターフェース
  – SVOM のサーバの設定
  – サーバマネージメントツール IPMIVIEW
  – BIOS 設定

  サーバの設定もしくは IPMIVIEW からスクリプトでの設定もできるため、ServerStart によるサーバの初期設定時に、iRMC S2 を設定できます。多数のサーバをスクリプトベースで設定することも可能です。

- CSS パネル（ローカルサービスパネル）のサポート
  PRIMERGY サーバに CSS パネル（ローカルサービスパネル）が付いている場合には、障害が発生したモジュールを特定して自分で交換することができます。

● ローカルユーザー管理

iRMC S2 には独自のユーザー管理機能があり、最大 16 ユーザーまでをパスワード付きで作成し、所属するユーザーグループに応じたさまざまな権限を摘要できます。

● ディレクトリサービスによるグローバルユーザー管理

iRMC S2 のグローバルユーザー ID は、ディレクトリサービスのディレクトリに集中保存されます。
サーバ上で集中管理されるユーザー ID は、ネットワーク上の全 iRMC S2 から共有されます。

次のディレクトリサービスをサポートしています。

– Microsoft® Active Directory
– Novell® eDirectory（未サポート）
– OpenLDAP

● DNS ／ DHCP

iRMC S2 では自動ネットワーク設定が可能です。初期値として設定されている名前と DHCP を使って、iRMC S2 は DHCP サーバから IP アドレスを受け取ります。iRMC S2 名は DNS（Domain Name Service：ドメインネームサービス）によって登録され、最大 5 つの DNS サーバがサポートされます。DNS/DHCP が利用できない場合は、静的 IP アドレスも使用できます。

● 電源ユニット

iRMC S2 は、電源ユニットのスタンバイ電源から電力が供給されます。

● 警告管理

iRMC S2 の警告通知（アラーティング）には、次の 3 種類があります。

– SNMP による PET（Platform Event Traps：プラットフォームイベントトラップ）送信
– E-mail による警告の直接送信
– モデム／シリアルインターフェース接続しての警告送信

また iRMC S2 は、あらゆる関連情報を ServerView エージェントへ提供します。

● SEL（System Event Log：システムイベントログ）の表示、フィルタリングおよび退避

次の方法で、SEL の内容を表示および退避し、削除できます。

– iRMC S2 Web インターフェースを利用
– iRMC S2 の Telnet/SSH ベースインターフェース（リモートマネージャ）を利用

iRMC S2 の拡張機能

iRMC S2 は、標準機能に加えて AVR およびリモートストレージ機能をサポートしています。

● AVR（Advanced Video Redirection：ビデオリダイレクション）iRMC S2 のビデオリダイレクションには、次のような利点があります。

– 標準 Web ブラウザによる操作。管理端末に Java 実行環境以外の追加ソフトウェアをインストールする必要がありません。

– システムから独立したグラフィカルおよびテキストコンソールのリダイレクション（マウスおよびキーボード含む）です。

– リモートアクセスによる起動監視および BIOS 管理、オペレーティングシステム操作が可能です。

– 異なる 2 箇所から 1 台のサーバに同時「仮想接続」しての作業が可能です。ハードウェア圧縮およびビデオ圧縮により、ネットワーク負荷も軽減されます。

– サーバ側のモニタの停止サポート。AVR セッション中のサーバ側の画面上で実行中のユーザー入力および作業が権限のない人間に見られることがないように、AVR セッション中に管理対象の PRIMERGY サーバ側の画面出力を停止することができます。

● リモートストレージ

リモートストレージにより、「仮想」ドライブが利用可能です。物理的にはリモート管理端末上に 存在している「仮想」ドライブを、リモートストレージサーバによりネットワーク使用します。

「仮想」ドライブとリモートストレージの組み合わせは、次のようにローカルドライブとほとんど 同じように使用できます。

– データの読み出しおよび書き込み
– リモートストレージからの起動
– ドライバおよび小規模アプリケーションのインストール
– リモート管理端末からの BIOS アップデート
（USB による BIOS アップデート）

リモートストレージは、リモート管理端末上の「仮想ドライブ」として、次のデバイスタイプをサ ポートしています。

– CD ROM
– DVD ROM
– メモリスティック
– フロッピーイメージ – CD ISO イメージ
– DVD ISO イメージ

また、リモートストレージサーバは、「仮想ドライブ」としてネットワーク上に ISO イメージを実現します。

リモートストレージでは、リモート管理端末に最大 2 つの「仮想」ドライブ同時接続を行うか、

リモートストレージサーバにより ISO イメージのプロヴィジョンを行うかが選択可能です。

1.3 iRMC S2 の操作インターフェース

iRMC S2 には、次の操作インターフェースがあります。

- **iRMC S2 Web インターフェース（Web インターフェース）**

  iRMC S2 Web サーバへは、Microsoft Internet Explorer もしくは Mozilla Firefox などの標準 Web ブラウザで接続します。

  iRMC S2 の Web インターフェースにより、あらゆるシステム情報およびファン速度や電圧などセンサからのデータへのアクセスを行います。また、テキストベースコンソールリダイレクションを 設定し、グラフィカルコンソールリダイレクション（AVR、Advanced Video Redirection）を開始します。さらに、管理者権限では、iRMC S2 Web インターフェースでの接続設定が可能です。iRMC S2 Web サーバへのアクセスは、HTTP ／ SSL によるセキュアなアクセスです。

  Web インターフェースによる iRMC S2 操作の詳細については、「7 章 iRMC S2 Web インターフェース」（→ P.209）を参照してください。

- リモートマネージャ：**LAN** によるテキストベース **Telnet/SSH** インターフェース

  リモートマネージャは、次の場所から起動できます。

  – ServerView Remote Management Frontend
  – Telnet/SSH クライアント

  リモートマネージャは、英数字インターフェースで、システム、センサ情報、電源管理機能および エラーイベントログへのアクセスを行います。さらに、テキストコンソールのリダイレクションもしくは SMASH CLP シェルを起動します。SSH（Secure Shell：セキュアシェル）をとおしてリモートマネージャを起動すると、リモートマネージャおよび管理対象サーバ間の接続は暗号化されます。

  リモートマネージャを利用した iRMC S2 操作の詳細については、「8 章 Telnet ／ SSH アクセス（Telnet ／ SSH での管理）」（→ P.361）を参照してください。

- リモートマネージャ（シリアル）：「シリアル **1**」によるテキストベースシリアルインターフェース

  リモートマネージャ（シリアル）は、リモートマネージャインターフェースと同じです。

1.4 IPMI のテクニカルな背景

iRMC S2 により、IPMI インターフェースから BMC 機能が利用可能です。

IPMP（Intelligent Platform Management Initiative）とは

IPMI は、複雑さを増す最新サーバシステムに対応するために生まれました。サーバシステム監視のための新しいソリューションをもとめて、多くのベンダーがこのイニシアティブに参加しています。

IPMI という名前が、ソリューションのアプローチの方向性を示しています。システムの監視機能およびリカバリ機能が、プラットフォーム管理ハードウェアおよびファームウェア上に直接実装されます。

IPMI の目的

IPMI は、システムを集中制御する BMC（Baseboard Management Controller : ベースボード管理コントローラ）とインテリジェントなプラットフォーム管理ハードウェアの間に、抽象化されたメッセージベースの標準インターフェースを実現することをめざしました。

IPMI は、さまざまなプラットフォーム管理モジュールの主要特性を、標準仕様としてまとめたもの なのです。

IPMI 規格

IPMI 規格仕様は、次のとおりです。

「IPMI は、特定の管理ソフトウェアに依存しないハードウェアレベルインターフェースの規格であり、監視および制御機能を DMI、WMI、CIM、SNMP などの標準管理ソフトウェアインタ ーフェースを通して提供する。ハードウェアレベルのインターフェースであるため、標準的な管 理ソフトウェアスタックの最下位に位置する。」「IPMI とその他の管理規格との関係」（→ P.19）を参照してください。

IPMI の利点

IPMI 仕様は、プロセッサもしくは BIOS、オペレーティングシステムごとのインベントリおよびログ、リカバリ、監視といった機能の独立性を保証します。

したがって、シャットダウンや電源遮断も、プラットフォームの管理のもとに行われます。

IPMI とその他の管理規格との関係

IPMI は、各オペレーティングシステム上のシステム管理ソフトウェアと連動して使用するのに最適です。IPMI の機能を管理アプリケーションおよびオペレーティングシステムの管理機能と組み合わせることによって、強力なプラットフォーム管理環境が実現します。

図 .2 に、IPMI および管理ソフトウェアスタックの関係の概要を示します。

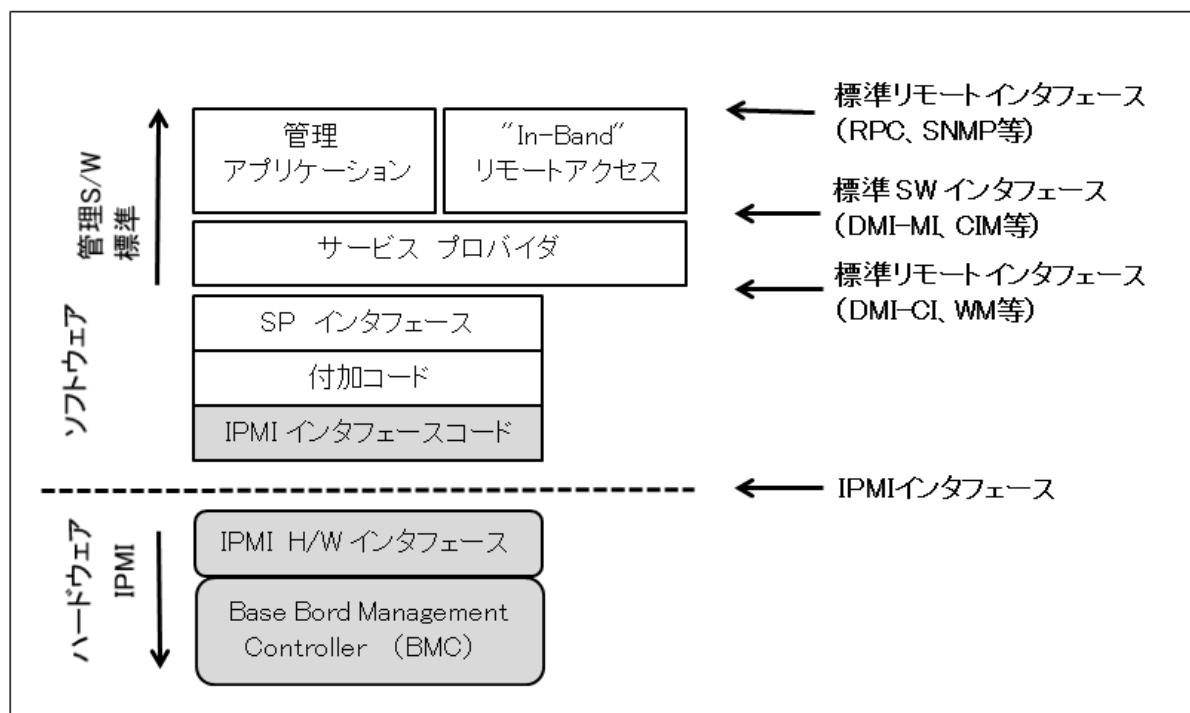



図 .2 : 管理ソフトウェアスタック上の IPMI の位置づけ （出典 : IPMI 規格、「引用」（→ P.24））

IPMI および IPMB、ICMB

IPMI イニシアティブの規格は、次の 3 つの仕様で構成されています。

– *IPMI*（*Intelligent Platform Management Interface*）IPMI ベースのシステムが実現するべき高レベルのアーキテクチャ、電流指令、イベントフォーマット、データパケット、およびさまざまな特性を規定しています。

– *IPMB*（*Intelligent Platform Management Bus*）プラットフォーム管理ハードウェアの内部モジュール間の標準接続のための I2C ベース（write only）バス仕様です。リモートマネジメントモジュールへの標準インターフェースとしても機能します。

– *ICMB*（*Intelligent Chassis Management Bus*）プラットフォーム管理情報のやりとり、および複数システムにまたがる制御を行う外部バスインタ ーフェースです。IPMB 接続するデバイス上で機能するようにデザインされています。ServerView リモートマネジメント環境では、まだ実装されていません。

IPMI の実装

IPMI 実装の中核となるのは、BMC（Baseboard Management Controller）です。BMC には、次の役割があります。

– システム管理ソフトウェアおよびプラットフォーム管理ハードウェア間のインターフェースのとりまとめ
– 監視およびイベントログ、リカバリ制御の自立機能の実現
– システム管理ソフトウェアおよび IPMB 間のゲートウェイとしての役割

IPMI を利用して管理コントローラを増設すれば、プラットフォーム管理の範囲が拡張します。IPMB は I2C ベースのシリアルバス仕様であり、管理コントローラ内部および管理コントローラ間の通信に使用されます。

IPIMI により、複数の管理コントローラと組み合わせた拡張性のあるアーキテクチャを実装できます。複数のコントローラにより､電源装置およびホットスワップ RAID ドライブモジュールなどの異なるサブシステムを監視する複雑なサーバシステムが構築できます。

IPMI には、IPMI コマンドを処理できない「インテリジェントでない」I2C モジュール上の IPMB に接続された管理コントローラをとおしてアクセスを行うための「低レベル」I2C コマンドもあります。

IPMI の基本構成要素の概要を図 .3（→ P.21）に示します。

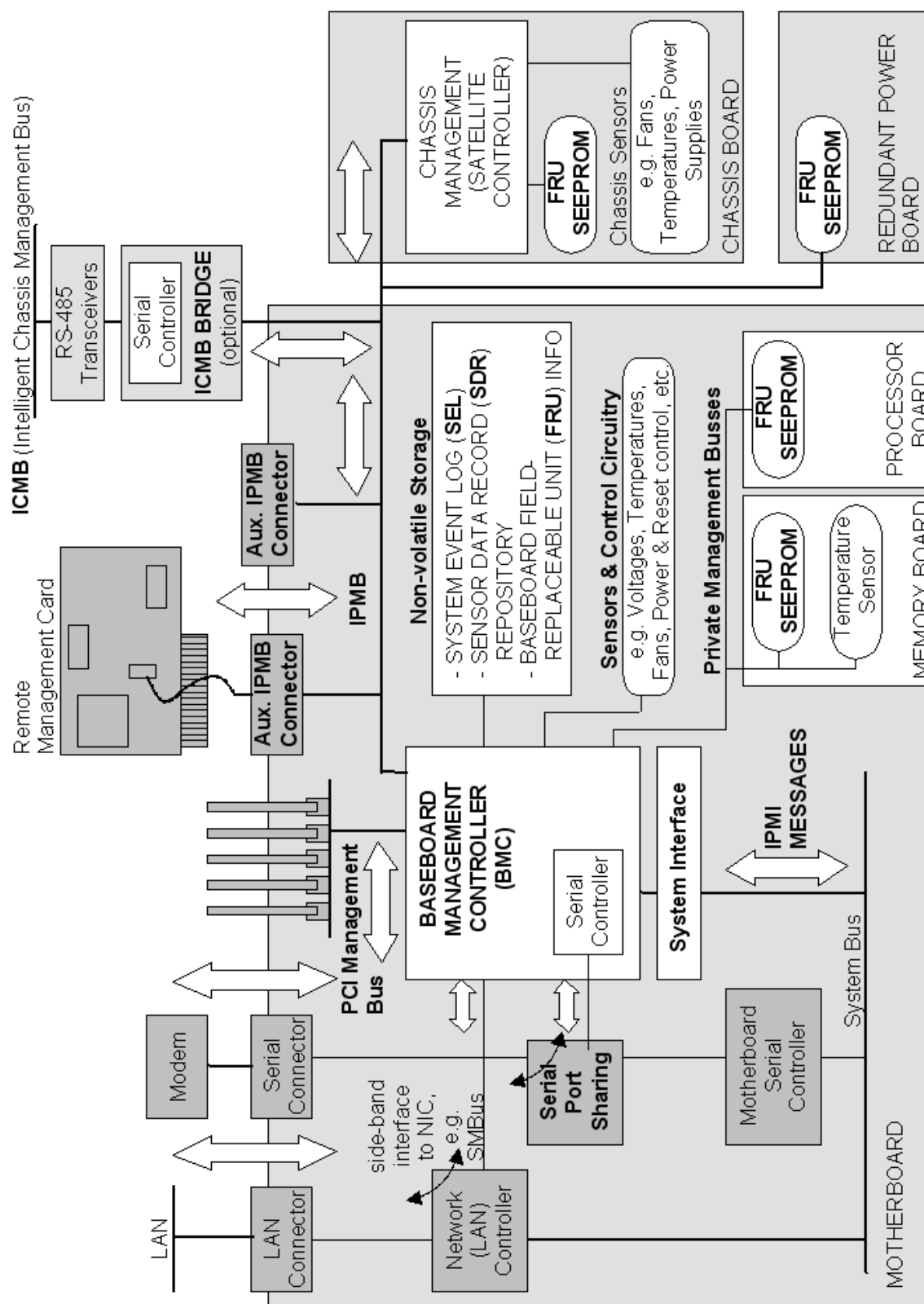



図 .3：IPMI ブロックダイアグラム（出典：IPMI 規格、「引用」（→ P.24））

IPMI と「In-bound」および「Out-bound」管理

システム管理の分野では、「In-bound」および「Out-bound」管理は次のように区別されます。

– 「In-bound」管理は、管理対象サーバ上でオペレーティングシステムが動作している場合の管理です。
– 「Out-bound」管理は、障害が発生したりして、管理対象サーバ上でオペレーティングシステムが動作していない場合の管理です。

IPMI 規格にしたがったシステム環境では異なるインターフェースが利用できるため、「In-bound」管理もしくは「Out-bound」管理のどちらにも対応します。

IPMI-over-LAN

IPMI-over-LAN は、IPMI 規格の LAN インターフェース仕様の新しい名称です。管理対象システムの BMC との間で IPMI メッセージを送りそして受け取る方法を規定する仕様で、RMCP（Remote Management Control Protocol : リモートマネジメント制御プロトコル）データパケットにカプセル化されます。RMCP データパケットは、イーサネット LAN 接続をとおして IPv4 UDP 転送されます。

もともと RMCP プロトコルは、オペレーティングシステムが動作していないシステム機器の管理のための規格であり、シンプルな問い合わせ／応答のプロトコルです。

BMC に適用されたオンボード LAN コントローラ上には、以上のような接続インターフェースがあります。

このインターフェースはオンボード LAN コントローラ上でのみ機能し、LAN カード上では機能しません。

UDP 下で RCMP が使用する 2 ポートのうち、BMC は LAN コントローラとの通信にポート 623（プライマリ RMCP ポート）使用します。

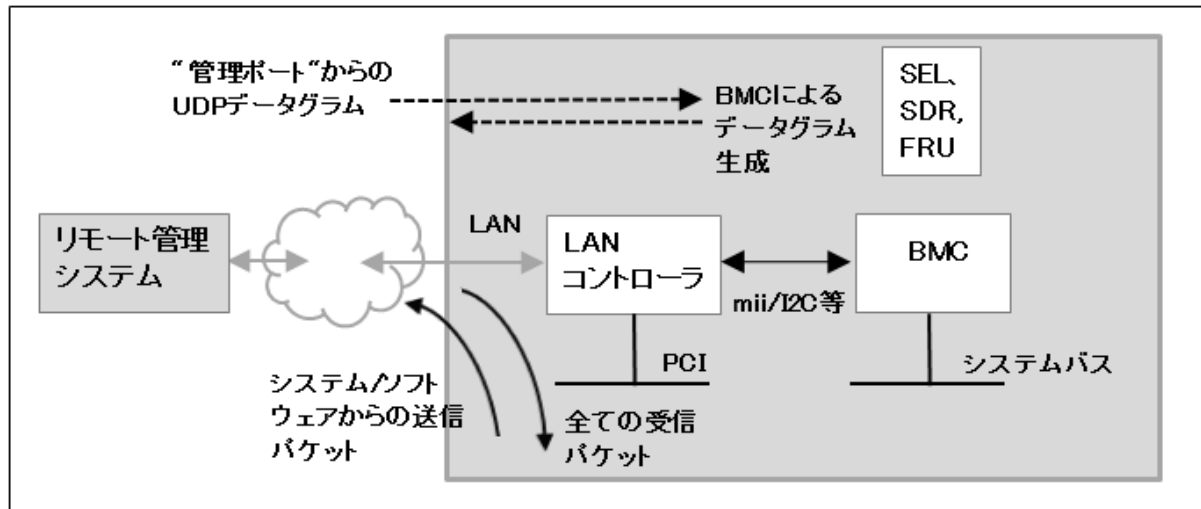



図 .4：BMC および LAN コントローラ

SOL（Serial Over LAN）インターフェース

SOL は IPMI V2.0 規格の一部であり、LAN 接続でのシリアルデータ転送のインターフェースです。特に、管理対象コンピュータのシリアルコントローラおよびリモート管理端末の間の LAN によるシリアルデータストリーム転送のパケットフォーマットおよびプロトコルを規定します。SOL は IPMI-over-LAN 仕様にもとづいています。

SOL 接続の確立には、まずリモートマネジメントアプリケーションが BMC との間に IPMI-over-LAN セッションを開始します。これが完了した段階で、リモート管理端末が SOL サービスを起動します。シリアルコントローラおよびリモート管理端末の間のデータトラフィックは、IPMI コマンドと同じ IPMI セッションで処理されます。

SOL 接続確立後すぐに、次のようにして、シリアルコントローラおよびリモート管理端末の間のデータ転送が行われます。

– シリアルコントローラからリモート管理端末への転送 シリアルコントローラからのデータストリームは BMC による分割後、圧縮されて LAN をとおして

  リモート管理端末に送られます。

– リモート管理端末からシリアルコントローラへの転送リモート管理端末から送られてきた圧縮文字列は

  BMC によって解凍され、文字ストリームとしてシ

  リアルコントローラに転送されます。

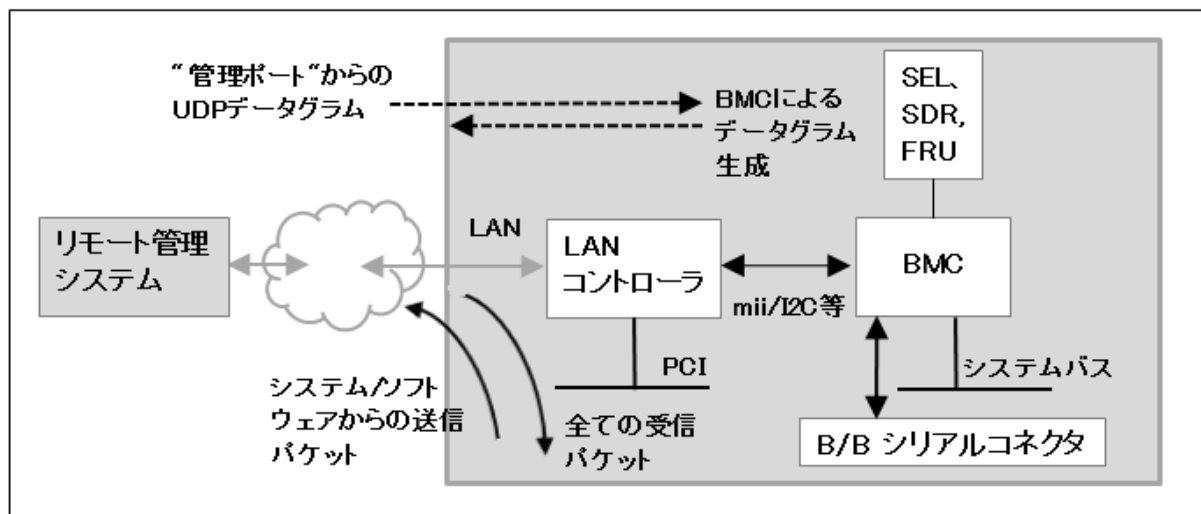



図 .5：BMC および SOL

管理対象システムおよびリモート管理端末の BMC 間の SOL メッセージとして、SOL 文字データが交換されます。SOL メッセージは RMCP+ データパケットにカプセル化され、IPv4 によりイーサネット LAN 接続をとおして UDP で転送されます。RMCP+ プロトコルは RMCP プロトコルにもとづ いていますが暗号化、認証などの拡張機能があります。
Serial over LAN では、管理対象サーバの BIOS もしくはオペレーティングシステムによるコンソールリダイレクションによる「ヘッドレス」管理が可能です。したがって、高価な集信装置は不要です。

IPMI のチャネルコンセプト

「チャネル」はさまざまな接続キャリアにより IPMI メッセージを BMC にルートするメカニズムであり、9 チャネルまでサポートされます。システムインターフェースおよびプライマリ IPMB は固定ですが残りの 7 チャネルは自由に実装できます。

チャネルには、「セッションベース」チャネルおよび「セッションレス」チャネルがあります。「セッション」のコンセプトには 、ユーザー認証のコンセプト（「ユーザーの識別」(→ P.24)）および単一チャンネルで複数の IPMI メッセージストリームをルーティングするためのコンセプトの 2 種類があります。

「セッションベース」チャネルの例には LAN チャネルもしくはシリアル／モデムチャネルがあり、「セッションレス」チャネルの例には、システムインターフェースおよび IPMB があります。

ユーザーの識別

「セッションベース」チャネル（「IPMI のチャネルコンセプト」(→ P.24)）では、ユーザーログ インが必要です。「セッションレス」チャネルでは、ユーザー認証の必要はありません。

IPMI では、ユーザー設定はチャネル単位です。つまり、LAN チャネルもしくはシリアルチャネルのどちらで BMC にアクセスしているかによって、ユーザーは異なる特権を持つことができます。

引用

IPMI 標準に関する情報は、次の Web サイトで見ることができます。（英語サイト）

http://developer.intel.com/design/servers/ipmi/index.htm

1.5 前バージョン以降の変更点

本バージョンは、以下のオンラインユーザーガイドに代わるものです。

『iRMC S2 - integrated Remote Management Controller, 2009 年 10 月版』

本ユーザーガイドには、以下の追加がなされています。

- 6 章「リモートストレージ」

  「Linux 環境でのリモートストレージ」が追加されました。

  表記されている画面およびイラストは一例であり、実際に表示される画面やイラスト、およびファイル名などが異なることがあります。
  また、このマニュアルに表記されているイラストは説明の都合上、本来接続されているケーブル類を省略していることがあります。

1.6 本文中の記号

本ユーザーガイドで使用している記号には、次の意味があります。

注意！	健康障害の兆候もしくはデータ消失やハードウェア障害にいたる可能性のある危険に対する注意を喚起
i	重要な情報およびヒント
▶	実行するべきアクション
イタリックテキスト	コマンドおよびメニュー項目、ボタン名、オプション名、ファイル名、パス名
< テキスト >	最新値で置き換えるべき変数
固定スペースフォント	システム出力
固定スペースフォント **太字固定スペースフォント**	キーボード入力するコマンドは太字の等幅フォント
[大括弧]	オプション項目
{ 中括弧 }	「 | 」で区切られた選択項目
[キーボード] [記号]	キーはキーボード記号で表示。大文字入力が必要な場合は、たとえば大文字の A に対して ［シフト］-［A］と表示 複数キーを同時に押す場合は、キーボード記号間をハイフンで結ぶ。

表 1：表記規約

本書内での引用箇所を示す場合は、参照するセクションの章名もしくは節名およびページ番号で示しています。

2 章 iRMC S2 初期設定接続

iRMC S2 の初期設定への接続は、一切の設定なしで行えます。

2.1 接続要件

リモート管理端末：

– Windows: Internet Explorer バージョン 6.x
  Linux: Mozilla Firefox 1.5
– コンソールリダイレクション：
  Sun Java Virtual Machine バージョン 1.5.0_06 以降

ネットワーク：

– ネットワーク上に DHCP サーバが必要です。
– IP アドレスではなく英字名で、iRMC S2 Web インターフェースにログインする場合、ネットワーク上の DHCP サーバはダイナミック DNS 設定されている必要があります。
– DNS の設定が必要です。設定していないと、IP アドレスを要求されます。

2.2 iRMC S2 の初期設定値

管理者 ID および iRMC S2 の DHCP 名の初期設定値は、iRMC S2 ファームウェアにあります。

管理者 ID の初期設定値

「管理者 ID」: admin

「パスワード」: admin

管理者 ID およびパスワードは、両方とも大文字と小文字を区別します。

セキュリティ上、最初のログイン後に新しい管理者アカウントを作成し、管理者アカウントの初期設定値は削除するようにしてください。最低でも、パスワードの変更は必ず行ってください。「7.13 ユーザー管理 – ユーザーの管理」→ P.311)を参照してください。

DHCP 取得 IP の DNS 登録名 初期設定値（iRMC S2）

DHCP 取得 IP の DNS 初期名（iRMC S2）は、次のフォーマットになっています。
「IRMC < シリアル番号 >」

シリアル番号は、iRMC S2 の MAC アドレスの最後の 3 バイトです。iRMC S2 の MAC アドレスは、使用している PRIMERGY サーバのラベルに記載されています。

ログイン後、iRMC S2 の MAC アドレスは、「ネットワークインターフェース」(→ P.290のページの欄上に read-only で表示されます。

2.3 iRMC S2 Web インターフェースでのログイン

➤ リモート管理端末上の Web ブラウザを開き、iRMC S2 の DNS 名もしくは IP アドレスを入力してください。

iRMC の DNS 名は使用している PRIMERGY サーバのラベルに記載されています。

次のログインプロンプトが表示されます。

図 .6：iRMC S2 Web インターフェースログインプロンプト

グインプロンプトが表示されない場合は、LAN の接続状態を確認してください。「3.1.4 LAN インターフェースのテスト」（→ P.37）を参照してください。

➤ アカウントの初期値を入力してください。
「ユーザー名」： admin
「パスワード」： admin

➤ ［OK］を押して確認してください。

iRMC S2 Web インターフェースについては、「システム情報ページ」（→ P.219）を参照してください。

3 章 iRMC S2 の設定

iRMC S2 の設定は、次のツールで行います。

– BIOS セットアップユーティリティ／ TrustedCore セットアップユーティリティ（→ P.35）
– RMC S2 Web インターフェース（→ P.209）
– サーバ設定（→ P.389）
– Server Management Tool （IPMIVIEW）

本章では、次の事項について説明しています。

– BIOS セットアップユーティリティによる iRMC S2 LAN インターフェースの設定（→ P.35）
– BIOS セットアップユーティリティによる LAN 経由テキストコンソールのリダイレクション（→ P.38）
– BIOS セットアップユーティリティによる iRMC S2 シリアルインターフェースの設定（→ P.45）
– Web インターフェースによる iRMC S2 の設定（→ P.49）
– サーバの設定 による iRMC S2 の設定（→ P.51）

3.1 iRMC S2 LAN インターフェースの設定

次の事項について説明しています。

– LAN インターフェースの必要条件

– BIOS セットアップユーティリティの LAN インターフェースの設定

– LAN インターフェースのテスト

iRMC S2 接続の「スパニングツリー」のツリーは、停止しておいてください。
（例：「Port Fast=enabled; Fast Forwarding=enabled」）

3.1.1 必要条件

IP アドレスの設定に関しては、次の点に注意する必要があります。

– LAN ケーブルが正しいポートに接続されている必要があります。「3.1.1.1 正しい LAN ポート への接続」（→ P.33）を参照してください。

– iRMC S2 およびシステムの IP アドレス間の相互動作。「iRMC S2 およびシステムの IP アドレス 間の相互動作」（→ P.34）を参照してください。

3.1.1.1 正しい LAN ポートへの接続

LAN 接続インターフェースは、iRMC S2 に適用されたオンボード LAN コントローラ上にあります。図 .4（→ P.23）を参照してください

PRIMERGY サーバには、システムボードの LAN インターフェースが 2 つのものと 3 つのものとがあります。レンチ記号がついているポートが、iRMC S2 用ポートです。図 .7 のポート 1 および左上のポートです。

LAN ケーブルが正しいポートに接続されていることを確認してください。

レンチ記号がついているポートは、PRIMERGY サーバによって異なります。

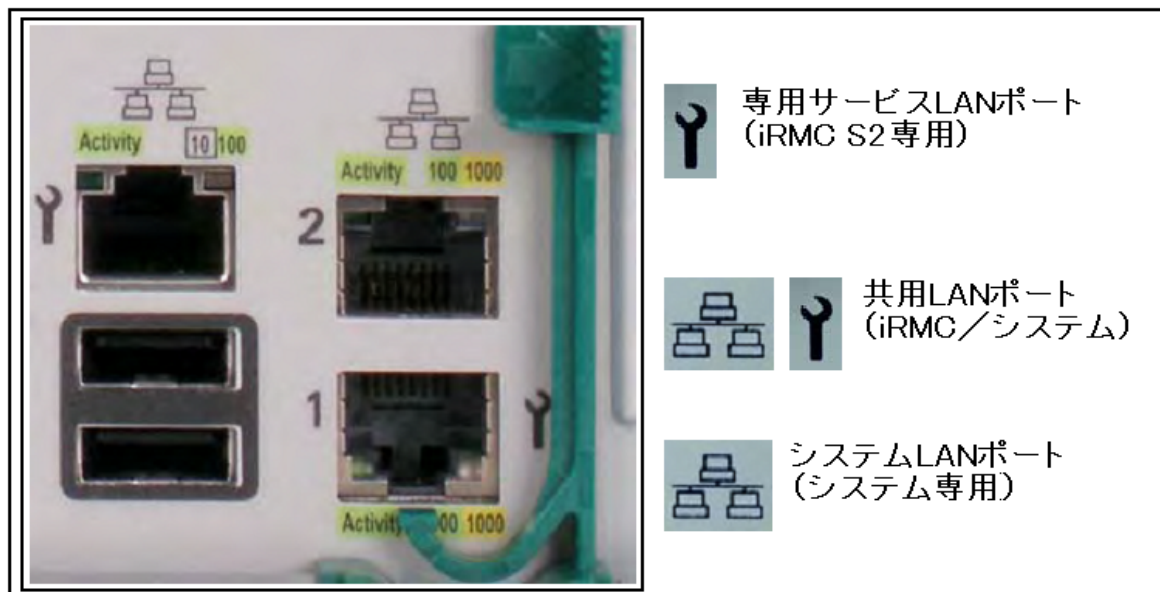



図 7：iRMC S2 用ポート（レンチ記号で示した箇所）

3.1.1.2 iRMC S2 およびシステムの IP アドレス間の相互動作

オペレーティングシステムではなく iRMC S2 に確実にデータパケットを転送するために、PRIMERGY サーバの LAN コントローラには、iRMC S2 専用の IP アドレスが必要です。

iRMC S2 の IP アドレスは、システム（オペレーティングシステム）とは別でなければなりません。

3.1.1.3 他のサブネットからのアクセス

リモート管理端末が、DHCP を使用しないで管理対象サーバの iRMC S2 に別サブネットからアクセスする場合、ゲートウェイを設定する必要があります。

3.1.2 LAN インターフェースの設定：Configuration tools

iRMC S2 の LAN インターフェースの設定には、いくつかの方法があります。

PRIMERGY サーバの機種によって、設定方法が異なります。

– BIOS セットアップユーティリティもしくは TrustedCore® セットアップユーティリティの使用（→ P.35）

– iRMC S2 Web インターフェースの使用。「7.11 ネットワーク設定— LAN パラメータの設定」（→ P.289）“ を参照してください。

– サーバ設定の使用。「9.6 iRMC LAN インターフェース iRMC S2 の LAN パラメータの設定」を参照してください。

– Server Management Tool の使用

3.1.3 BIOS ／ TrustedCore セットアップユーティリティによる LAN インター フェースの設定

➢ 管理サーバの BIOS / TrustedCore セットアップユーティリティを起動します。サーバの起動時に［F2］を押してください。

➢ LAN パラメータ設定メニューを起動します。

– BIOS :「Advanced」–「IPMI」– 「LAN Setting」

– TrustedCore :「Server」–「IPMI」–「LAN Setting」

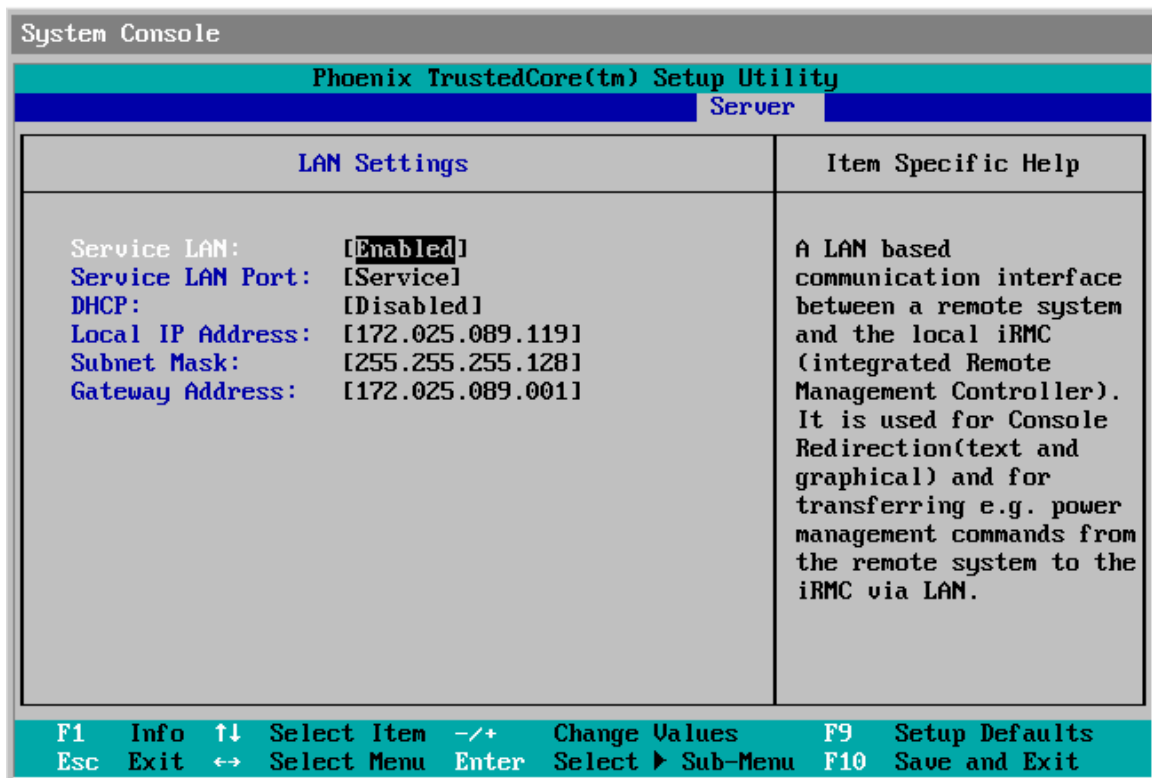



図 8 : LAN 設定メニュー（TrustedCore セットアップユーティリティの場合）

➢ 次の設定を行ってください。

「*Service LAN*」
　　「*Enabled*」に設定してください。

「*Service LAN Port*」
　　「*Service*」に設定することを推奨します。

ℹ TX150 S6 PRIMERGY の場合は、必ず「Service」に設定してください。

「*DHCP*」

DHCP を有効にした場合、iRMC S2 の LAN 設定はネットワーク上の DHCP サーバから自動的に行われます。「*Local IP Address*」、「*Subnet Mask*」などの値も自動的に設定されます。

利用できる DHCP サーバがない場合には、DHCP オプションを有効にしないでください。iRMC S2 は常時 DHCP サーバをサーチしており、利用できる DHCP サーバがない場合に DHCP オプションを有効にするとサーチがループします。

初期インストール後に、iRMC S2 Web インターフェースから DHCP および DNS サービスの利用を指定できます。これについては、「7.11.3 DHCP 設定 — iRMC S2 のホスト名の設定」（→ P.297）および「7.11.4 DNS 設定— iRMC S2 の DNS 使用の有効化」（→ P.299）を参照してください。

何も指定しない場合、iRMC S2 の初期インストール時に DHCP サーバには次の名前がわたされます :「*iRMC* ＜ *MAC* アドレスの最後の *3* バイト＞」。

「*Local IP Address*」
管理するシステムの iRMC S2 の IP アドレスを入力します。

「*Subnet Mask*」
ネットワークのサブネットマスクを入力します。

「*Gateway Address*」
ゲートウェイの IP アドレスを入力します。

- 設定を保存します。
- iRMC S2 のコンソールリダイレクションを使用する場合は、「3.2 BIOS / TrustedCore セットアップユーティリティによる LAN をとおしたテキストコンソールのリダイレクションの設定」（→ P.38）の記述にしたがって設定を続けてください。

iRMC S2 のテキストコンソールのリダイレクションを使用しない場合は、BIOS/TrustedCore 設定を終了し、「3.1.4 LAN インターフェースのテスト」（→ P.37）の記述にしたがって設定を続けてください。

3.1.4 LAN インターフェースのテスト

次の手順で、LAN インターフェースをテストします。

➢ Web ブラウザから、iRMC S2 Web インターフェースにログインしてください。ログインプロンプトが表示されない場合には、LAN インターフェースが動作していない可能性があります。

➢ Ping コマンドで、iRMC S2 接続をテストしてください。

3.2 BIOS/TrustedCore セットアップユーティリティによる LAN を経由したテキストコンソールのリダイレクションの設定

テキストコンソールのリダイレクション設定およびサーバのオペレーティングシステムにより、テキストコンソールのリダイレクションには 2 種類の利用方法があります。

– BIOS POST フェーズ終了時にテキストコンソールのリダイレクションを停止する。

– BIOS POST フェーズ終了後も、オペレーティングシステムが稼働している間はテキストコンソールのリダイレクションが利用可能である。

本節では、次の事項を説明します。

– BIOS ／ TrustedCore セットアップユーティリティによる LAN をとおしたテキストコンソールのリダイレクションの設定

– オペレーティングシステムの稼働中にコンソールリダイレクションを行う場合に考慮するべきオペレーティングシステムの特別な必要条件

i iRMC S2 Web インターフェースからも LAN をとおしたテキストコンソールのリダイレクションを設定できます。「7.14.1 BIOS テキストコンソール—テキストコンソールの リダイレクションの設定と開始」（→ P.333）を参照してください。

3.2.1 テキストコンソールのリダイレクション設定

➢ 管理対象サーバの BIOS ／ TrustedCore セットアップユーティリティを起動します。サーバの起動中に［F2］を押してください。

Peripheral Configuration Menu 設定

➢ Peripheral Configuration Menu を起動します。

「*Advanced*」－ 「*Peripheral Configuration*」

```
System Console
Phoenix TrustedCore(tm) Setup Utility
Advanced

Peripheral Configuration                  Item Specific Help

Serial 1:              [Enabled]          Selects which device
  Serial 1 Address:    [3F8/IRQ 4]        uses the shared serial
Serial Multiplexer:    [iRMC]             port.

  USB Front:           [Enabled]
  USB Rear:            [Enabled]
  USB Devices:         [All]

LAN Controller:        [LAN 1 & 2]
LAN 1 Oprom:           [PXE]
LAN 2 Oprom:           [Disabled]

F1  Info  ↑↓ Select Item  -/+   Change Values       F9  Setup Defaults
Esc Exit  ↔  Select Menu  Enter Select ▶ Sub-Menu   F10 Save and Exit
```

図 9：周辺機器設定メニュー（TrustedCore セットアップユーティリティ表示）

➢ 次の設定を行ってください。

「*Serial 1*」

「*Enabled*」に設定してください。

「*Serial 1 Address*

最初に表示されたペア値を使用してください。

「*Serial Multiplexer*」

「*iRMC*」に設定してください。

Console Redirection Menu 設定

➢ Console Redirection Menu を起動してください。

「*Server*」–「*Console Redirection*」

i　表示される Console Direction Menu のイメージは、ご使用のセットアップユーティリティ（BIOS もしくは TrustedCore）によって異なります。

➢ **BIOS** セットアップユーティリティで次の設定を行ってください。

図 10：コンソールリダイレクションメニュー（BIOS セットアップユーティリティ表示）

「*Console Redirection*」
　「*Enabled*」に設定してください。

「*Port*」
　「*Serial 1*」に設定してください。

「*Baud Rate*」
　ボーレートを指定してください。

「*Protocol*」
　設定を変更しないでください（使用しているターミナルによって異なります）。

「*Flow Control*」

設定を変更しないでください（使用しているターミナルによって異なります）。

「*Mode*」

POST フェーズ終了後、オペレーティングシステム稼働中のコンソールリダイレクションの動作を指定します。「3.2.2 オペレーティングシステム稼働中のコンソールリダイレ クションの使用」（→ P.43）を参照してください。

「*Standard*」

BIOS POST フェーズ終了時にコンソールリダイレクションを停止します。

「*Enhanced*」

BIOS POST フェーズ終了後もコンソールリダイレクションを利用できます。

➢ **TrustedCore** セットアップユーティリティで次の設定を行ってください。

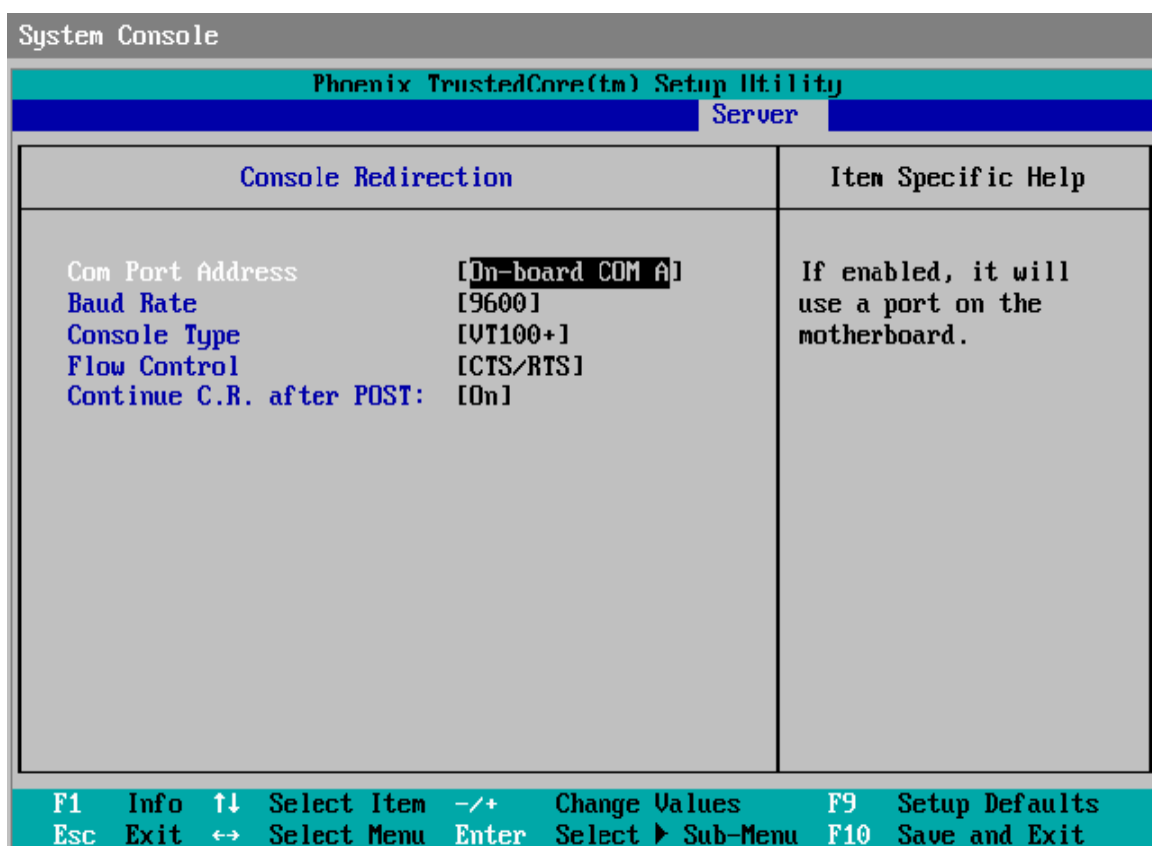



図 11：コンソールリダイレクションメニュー（TrustedCore セットアップユーティリティ表示）

「*Com Port Address*」

「On-board COM A」に設定してください。

「*Baud Rate*」

ボーレートを指定してください。

「*Console Type*」
設定を変更しないでください（ご使用のターミナルによって異なります）。

「*Flow Control*」
設定を変更しないでください（ご使用のターミナルによって異なります）。

「*Continue C.R. after POST*」
POST フェーズ終了後、オペレーティングシステム稼働中のコンソールリダイレクションの動作を指定します。「3.2.2 オペレーティングシステム稼働中のコンソールリダイレ クションの使用」（→ P.43）を参照してください。

「*Off*」
BIOS POST フェーズ終了時にコンソールリダイレクションを停止します。

「*On*」
BIOS POST フェーズ終了後もコンソールリダイレクションを利用できます。

BIOS / TrustedCore セットアップの終了

➢ 設定を保存して、BIOS/TrustedCore セットアップユーティリティを終了してください。

➢ 「3.1.4 LAN インターフェースのテスト」（→ P.37）の記述に従って設定を続行してください。

3.2.2 OS 動作中のコンソールリダイレクションの使用

管理対象サーバのオペレーティングシステムによっては、BIOS POST フェーズの終了後もコンソールリダイレクションを使用することができます。

DOS

コンソールリダイレクションモードの BIOS 設定は、次のように行ってください。「コンソールリダ イレクションメニュー設定」（→ P.40）を参照してください。

– BIOS セットアップユーティリティ :「Mode: Enhanced」
– TrustedCore セットアップユーティリティ :「Continue C.R. after POST: On」

Windows Server 2003

Windows Server 2003 では、POST フェーズの終了後、コンソールリダイレクションは自動的に処理されます。設定は一切不要です。オペレーティングシステム起動中は、Windows Server 2003 SAC コンソールが転送されます。

図 .12 : Windows Server 2003 SAC コンソール

Linux

POST フェーズの終了後もコンソールリダイレクションを処理するように、Linux オペレーティングシステムを設定する必要があります。設定すれば、リモート管理端末から無制限にアクセスできます。

設定項目

プログラムのバージョンによって設定が異なります。

SuSE および *RedHat*（*SuSE* は未サポート）

次の行を、*/etc/inittab* ファイルの最後に追加してください。
「xx:12345:respawn:/sbin/agetty < ボーレート > ttyS0」

RedHat

次のカーネル起動パラメータを */etc/grub.conf* ファイルに追加してください。
「console=ttyS0,< ボーレート > console=tty0」

SuSE（未サポート）

次のカーネル起動パラメータを */boot/grub/menu.lst* ファイルに追加してください。
「console=ttyS0,<baud-rate> console=tty0」

3.3 iRMC S2 シリアルインターフェースの設定および使用

iRMC S2 のシリアルインターフェースでは、次のことが可能です。

– ヌルモデムケーブル（RS-232C　のクロスケーブル）により端末アプリケーションリモートマネージャ（シリアル）を使用できます。「リモートマネージャ（シリアル）インターフェースの使用」（→ P.48）を参照してください。

– モデムにより警告を転送できます。iRMC S2 の Web インターフェースから設定します。「7.12.2 シ リアル／モデムによる通知—モデムを通した通知の設定」（→ P.303）を参照してください。

3.3.1 シリアルインターフェースの設定

BIOS の設定

- 管理対象サーバの BIOS ／ TrustedCore セットアップユーティリティを起動します。サーバの起動中に［F2］を押してください。
- Peripheral Configuration Menu（周辺機器設定メニュー）を起動してシリアルポートを設定してください。

「*Advanced*」–「*Peripheral Configuration*」

```
System Console
                 Phoenix TrustedCore(tm) Setup Utility
            Advanced
           Peripheral Configuration               Item Specific Help

  Serial 1:              [Enabled]               Selects which device
    Serial 1 Address:    [3F8/IRQ 4]             uses the shared serial
  Serial Multiplexer:    [iRMC]                  port.

    USB Front:           [Enabled]
    USB Rear:            [Enabled]
    USB Devices:         [All]

  LAN Controller:        [LAN 1 & 2]
  LAN 1 Oprom:           [PXE]
  LAN 2 Oprom:           [Disabled]

 F1   Info  ↑↓  Select Item  -/+    Change Values        F9   Setup Defaults
 Esc  Exit  ↔   Select Menu  Enter  Select ▶ Sub-Menu    F10  Save and Exit
```

図 .13：周辺機器設定メニュー（TrustedCore セットアップユーティリティ表示）

- 次の設定を行ってください。

「*Serial 1*」
　　「Enabled」に設定してください。

「*Serial 1 Address*」
　　最初に表示されたペア値を使用してください。

「*Serial Multiplexer*」
　　iRMC に設定してください。

次の値はメニューには表示されませんが、事前に設定されています。「端末プログラム（VT100+）」（→ P.48）を参照してください。

「*Bits per second*」
　9600 に設定してください。

「*Data bits*」
　8 に設定してください。

「*Parity*」
　「*None*」に設定してください。

「*Stop bits*」
　1 に設定してください。

「*Flow Control*」
　「*None*」に設定してください。

BIOS ／ TrustedCore セットアップの終了

➢ 設定を保存して、BIOS ／ TrustedCore セットアップユーティリティを終了してください。

➢ 「3.1.4 LAN インターフェースのテスト」（→ P.37）の記述に従って設定を続行してください。

3.3.2 シリアル接続管理インターフェースの利用方法

ヌルモデムケーブルでコンピュータを接続して端末プログラム（VT100+）を開始すると、シリアル接続端末プログラムにアクセスできます。シリアル接続管理インターフェースは、リモートマネージャインターフェースとまったく同じです。「8 章 Telnet ／ SSH アクセス（Telnet ／ SSH での管理）」（→ P.361）を参照してください。

前提条件

管理対象サーバ：

iRMC 上の「Serial Multiplexer BIOS」を設定する必要があります。「3.3.1 シリアルイン ターフェースの設定」（→ P.46）を参照してください。

端末プログラム（VT100+）：

次のように、端末プログラムのポートセッティングを行ってください。

「*Bits per second*」
9600 に設定してください。

「*Data bits*」
8 に設定してください。

「*Parity*」
「None」に設定してください。

「*Stop bits*」
1 に設定してください。

「*Flow Control*」
「None」に設定してください。

3.4 iRMC S2 の Web インターフェースの設定

➢ iRMC S2 Web インターフェースを起動してください。「7.1 iRMC S2 Web インターフェースへ のログイン」（→ P.210）を参照してください。

3.4.1 LAN パラメータ設定

➢ ナビゲーション領域の ［ネットワーク設定］をクリックしてください。「7.11 ネットワーク設定 — LAN パラメータの設定」（→ P.289）を参照してください。

LAN の設定

➢ 「ネットワークインターフェース」のページで LAN 設定を行ってください。設定の詳細については、「7.11.1 ネットワークインターフェース iRMC S2 に関するイーサネット設定」（→ P.290）を参照してください。

ポートとネットワークサービスの設定

➢ 「ポートとネットワークサービス」のページでポートおよびネットワークサービスを設定してください。設定の詳細については、「7.11.2 ポート番号とネットワークサービス—ポート番号とネ ットワークサービスの設定」（→ P.293）を参照してください。

DHCP 設定

➢ 「DHCP 設定」のページで DHCP の設定を行ってください。設定の詳細については、「7.11.3 DHCP 設定— iRMC S2 のホスト名の設定」（→ P.297）を参照してください。

DNS 設定

➢ 「DNS 設定」のページで DNS の設定を行ってください。設定の詳細については、「7.11.4 DNS 設定— iRMC S2 の DNS 使用の有効化」（→ P.299）を参照してください。

3.4.2 通知の設定

通知設定のページは、ナビゲーション領域の 「通知情報設定」にまとめられています。「7.12 警告 通知―警告通知の設定」(→ P.301)を参照してください。

SNMP による通知送信の設定

- ナビゲーション領域の「SNMP トラップ」をクリックしてください。「SNMP トラップ」のページが表示されます。
- SNMP トラップ送信を設定してください。設定の詳細については、「7.12.1 SNMP トラップ通知 ― SNMP トラップ通知の設定」(→ P.302)を参照してください。

モデムによる携帯電話への送信の設定(未サポート)

- ナビゲーション領域の[シリアル/モデム」をクリックしてください。「シリアル/モデム通知」のページが表示されます。
- モデムによる送信を設定してください。設定の詳細については、「7.12.2 シリアル/モデムによる通知―モデムを通した通知の設定」(→ P.303)を参照してください。

E-mail 通知の設定(**E-mail** による通知)

- ナビゲーション領域の「Email」をクリックしてください。「E-mail 通知」のページが表示されます。
- E-mail 通知を設定してください。設定の詳細については、「7.12.3 E-mail による通知― E-mail による通知の設定」(→ P.305)を参照してください。

3.4.3 テキストコンソールのリダイレクションの設定

- 「BIOS テキストコンソール」ウィンドウで、テキストコンソールのリダイレクションを設定してください。設定の詳細については、「7.14.1 BIOS テキストコンソール―テキストコンソールのリ ダイレクションの設定と開始」(→ P.333)を参照してください。

3.5 サーバの設定を使用した iRMC S2 の設定

➢ サーバ設定 を開始してください。「9 章 サーバの設定を使用した iRMC S2 設定」(→ P.389)を参照してください。

3.5.1 LAN パラメータの設定

LAN の設定

➢ 「iRMC LAN インターフェース」ダイアログボックスで LAN 設定を行ってください。設定の詳細については、「9.6 iRMC LAN インターフェース iRMC S2 の LAN パラメータ設定」(→ P.406)を参照してください。

ポートおよびネットワークサービスの設定

➢ 「iRMC ネットワークポート」ダイアログボックスでポートおよびネットワークサービスの設定を行ってください。設定の詳細については、「9.7 iRMC ネットワーク用ポート―ポート番号とネットワークサービスの設定」(→ P.409)を参照してください。

DHCP ／ DNS(dynamic DNS : ダイナミック DNS)の設定

➢ 「iRMC DNS 登録」ダイアログボックスで DHCP 設定を行ってください。設定の詳細については、「9.8 iRMC DNS 登録― iRMC S2 のホスト名のサーバの設定を使った設定」(→ P.411)を参照 してください。

DNS の設定

➢ 「iRMC DNS サーバ」ダイアログボックスで DNS 設定を行ってください。設定の詳細については、「9.9 iRMC DNS サーバ― iRMC S2 の DNS の有効化」(→ P.413)を参照してください。

3.5.2 通知の設定

SNMP による通知送信の設定

➢ 「iRMC SNMP トラップ」ダイアログボックスで SNMP トラップ送信の設定を行ってください。設定の詳細については、「9.12 iRMC SNMP トラップ―設定 SNMP トラップ警告」（→ P.420）を参照してください。

E-mail 通知の設定（**E-mail** による通知）

➢ 「iRMC E-mail 送信」ダイアログボックスでディレクトリサービスの E-mail 設定を行ってください。設定の詳細については、「9.10 iRMC E-mail 送信― E-mail 警告の設定」（→ P.415）を参照してください。

➢ 「iRMC E-mail 送信フォーマット」ダイアログボックスで Email のフォーマット設定を行ってください。設定の詳細については、「9.11 iRMC E-mail 送信フォーマット― E-mail 送信フォーマットの設定」（→ P.418）を参照してください。

4 章 iRMC S2 によるユーザー管理

iRMC S2 によるユーザー管理には 2 種類のことなるユーザー ID を使用します。

– ローカルユーザー ID は、iRMC S2 内部の不揮発性記憶装置に保存され、iRMC S2 のユーザーインターフェース経由で管理されます。

– グローバルユーザー ID はディレクトリサービスの集中データストアに保存され、ディレクトリサービスのインターフェース経由で管理されます。

グローバル iRMC S2 ユーザー管理では、現在以下のディレクトリサービスがサポートされます。

– Microsoft® Active Directory
– Novell® eDirectory（未サポート）
– OpenLDAP

本章では以下について説明します。

– iRMC S2 によるユーザー管理の概念
– ユーザー許可
– iRMC S2 上のローカルユーザー管理
– 個別のディレクトリサービスを使用するグローバルユーザー管理

4.1 iRMC S2 によるユーザー管理の概念

iRMC S2 によるユーザー管理は、ローカルとグローバルのユーザー ID を並列に管理することができます。

ユーザーがいずれかの iRMC S2 のインターフェースにログインするために入力する認証データ（ユーザー名、パスワード）を検証する際には、iRMC S2 は以下のように処理します（合わせて 55 ページの図 14 も参照してください）。

1. iRMC S2 はユーザー名とパスワードを内部に保存されたユーザー ID と照合します。
   - ユーザーは、iRMC S2 認証に成功すれば（ユーザー名とパスワードが有効）ログインすることができます。
   - 認証に失敗した場合には、iRMC S2 は成功するまで繰り返すか、（設定がある場合）LDAP での認証を行います。
2. iRMC S2 はユーザー名とパスワードを使用して、LDAP 経由でディレクトリサービスの認証を受け、LDAP クエリによってユーザーの権限を判断してユーザーに、iRMC S2 を操作する権限があるかどうかを確認します。

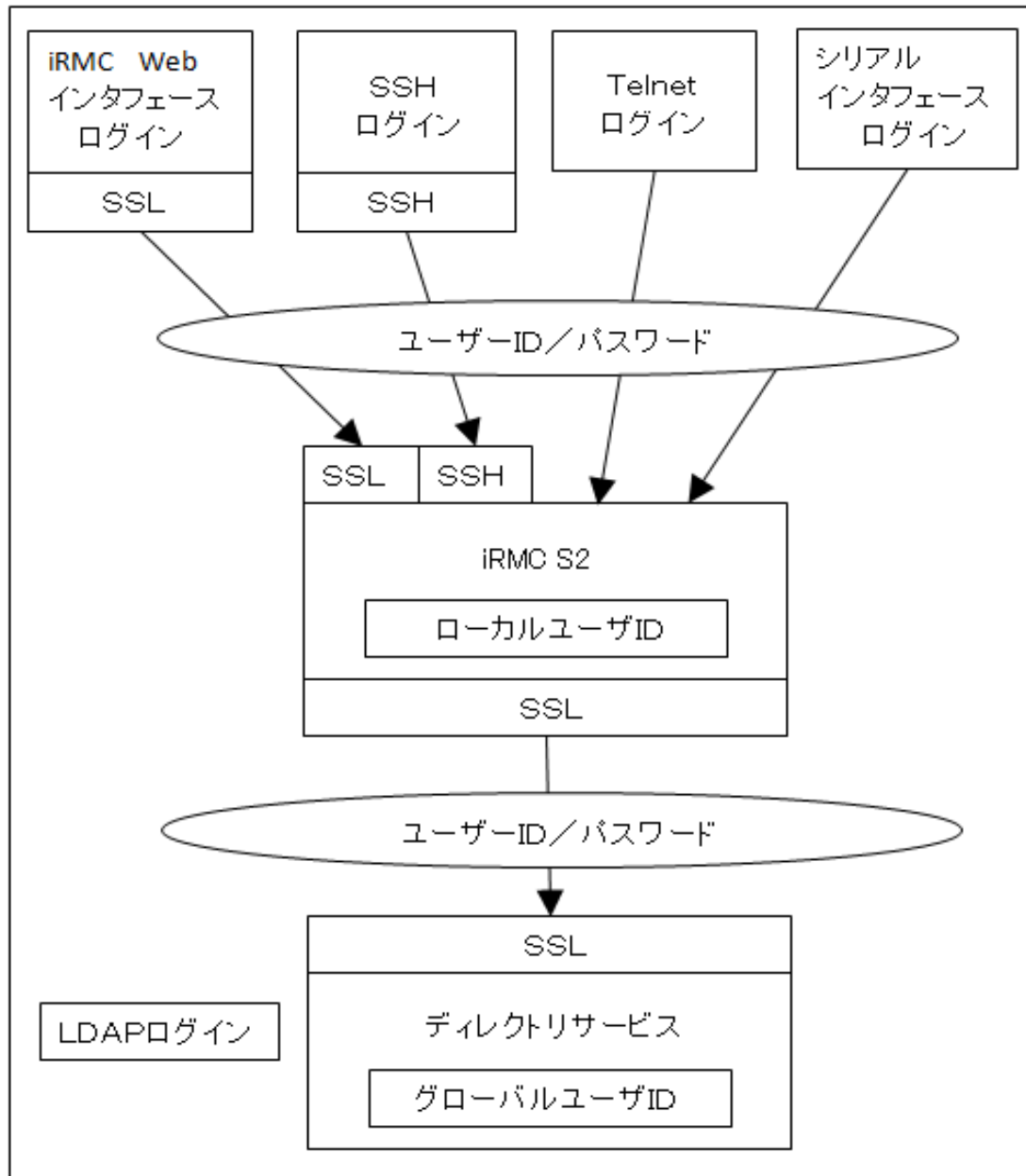



図 14： iRMC S2 経由のログイン認証

iRMC S2 とディレクトリサービスの間の LDAP 接続には、オプションの SSL を使用することを推奨します。SSL で保護された iRMC S2 とディレクトリサービスの間の LDAP 接続では安全なデータ交換が保証されますが、特にユーザー名とパスワードのデータの送信が安全にできます。

iRMC S2 Web インターフェース経由の SSL ログインが必要になるのは、LDAP が有効な場合のみです（LDAP 有効化オプション、322 ページを参照してください）。

4.2 ユーザー権限

iRMC S2 は以下の 2 つの相互補完的なユーザー権限を区別します。

– 接続経路別の権限（LAN ／シリアル接続の許可グループ割り当て）

– iRMC S2 独自の機能によるアクセス許可

個々の iRMC S2 機能を使用するために必要な特権と許可は次の通りです。

– iRMC S2 – Web インターフェース間に関しては 212 ページ参照

– リモートマネージャに関しては 370 ページ参照

接続経路別の権限（LAN ／シリアルの許可グループ)

iRMC S2 は各々のユーザー ID を次の 4 つの LAN ／シリアル接続許可グループのうちのひとつに割り当てます。

– User
– Operator
– Administrator
– OEM

iRMC S2 はこれらの許可を、チャンネル固有を基本にして割り当てますので、ユーザーは、iRMC S2 に LAN のインターフェースを経由して接続したか、シリアルインターフェースを経由して接続したかにより、別々に許可を取得することができます。

与えられる許可の範囲は、「User」（最も低い許可レベル）から 「*Operator*」、「*Administrator*」、「*OEM*」（最も高い許可レベル）の順に大きくなります。

許可グループは IPMI 特権レベルに対応しています。特定の許可（たとえば、「*Power Management*」）はこれらのグループまたは特権レベルに関連づけられます。

iRMC S2 独自の機能による許可

接続経路別の許可に加えて、ユーザーに次の許可を個別に割り当てることもできます。

– ユーザーカウントの設定

ローカルユーザー ID を設定する許可

– iRMC S2 設定の設定

iRMC S2 設定の設定する許可

– Video Redirection 許可

アドバンストビデオリダイレクション（AVR）を「「ビューモード」、「フルコントロールモード」で使用する許可

– リモートストレージ許可

リモートストレージ機能を使用する許可

初期設定のユーザー ID

iRMC S2 のファームウェアには、iRMC S2 用のすべての許可を持つデフォルトの管理者 ID が用意されています。

管理者 ID ： admin

パスワード ： admin

ローカルユーザーの場合には管理者 ID もパスワードも大文字小文字を区別します。最初にログインした時になるべく早く新しい管理者アカウントを作成して、デフォルトの管理者アカウントを削除するか、少なくともパスワードを変更しておくことを強く推奨します。
（311 ページ、「ユーザー管理－ユーザーの管理」の節を参照してください。）

4.3 iRMC S2 のローカルユーザー管理

iRMC S2 には 2 種類のローカルユーザー管理方法があります。最大 16 人のユーザーをパスワード付きで設定し、それぞれが属するユーザーグループによってさまざまな権限を割り当てることができます。ユーザー ID は、iRMC S2 内部の不揮発性記憶装置に保存されます。ユーザー管理はスクリプト（IPMIView 使用）によりマニュアルで操作することができます。

iRMC S2 上のユーザー管理には次のオプションが使用可能です。

– WebWeb インターフェース経由のユーザー管理

– Server Configuration Manager 経由のユーザー管理

– Server Management Tool （IPMIVIEW）経由のユーザー管理

4.3.1 iRMC S2 Web インターフェースによるローカルユーザー管理

i　iRMC S2 上のユーザー管理には「Configure User Accounts」許可が必要です。

設定されたユーザーのリストは Web インターフェースの下に見ることができます。新しいユーザーの設定、既存ユーザーの設定変更、または、ユーザーのリストからの削除が可能です。

➢ iRMC S2 の Web インターフェースを起動します（210 ページの「iRMC S2 Web インターフェー スへのログイン」の節を参照してください。）

設定されたユーザーのリスト表示

➢ ナビゲーション領域で「ユーザー管理」-「iRMC S2 ユーザー管理」をクリックします。

「iRMC S2 ユーザー情報 」ページが開いて設定されたユーザーのリストが表示されます（311 ペー ジを参照してください）。ここで、ユーザーの削除と新しいユーザーの設定ができます。

ユーザー管理のページに関しては 311 ページの「ユーザー管理－ユーザーの管理」の節に説明があります。

新しいユーザーの設定

➢ 「iRMC S2 ユーザー情報」ページで ［ユーザーの新規作成］ボタンをクリックします。

「新規ユーザーの構成」ページが開きます。このページで新しいユーザーの基本設定を設定することができます。このページに関しては 313 ページの「新規ユーザーの構成 – 新規ユーザーの設定」の節に説明があります。

ユーザーの設定変更

➢ 「iRMC S2 ユーザー情報 」のページで、設定されたパラメータを変更したいユーザーのユーザー名をクリックします。

ユーザー〈name〉の設定 ページが開いて選択されたユーザーの設定値を表示します。このページで新しいユーザーの設定パラメータを変更することもできます。ユーザー〈*name*〉の設定のページに関しては 314 ページの「User “<name>” Configuration - User configuration (details)」の節に説明があります。

ユーザーの削除

➢ 「iRMC S2 ユーザー情報」ページで削除するユーザーと同じ行にある［削除］ボタンをクリックします。

4.3.2 サーバの設定でのローカルユーザー管理

前提条件：

管理対象サーバには最新の 「ServerView」エージェントをインストールしておく必要 があります。

iRMC S2 上のユーザー管理には「ユーザーアカウント構成」許可が必要です。

設定されたユーザーのリストは「Server Configuration Manager」の下で見ることができます。新しいユーザーの設定、既存ユーザーの設定変更、または、ユーザーのリストからの削除が可能です。

➢ Server Configuration Manager を起動します （389 ページ、「サーバの設定を使用した iRMC S2 設定」の章を参照してください）。

設定されたユーザーのリスト表示

➢ 「iRMC ユーザー管理」を選択します。

このダイアログボックスには設定されたすべてのユーザーが含まれています（421 ページを参照してください。）

ここでユーザーを削除し「ユーザーの修正」ウィンドウを開いて選択したユーザーの設定を表示させることができます。

このウィンドウに関する説明は 422 ページにあります。

新しいユーザーの設定

➢ 「iRMC ユーザー管理」ダイアログボックスでユーザー ID のみが表示されているユーザーの 1 行下を選択します。

➢ ［修正］ボタンをクリックし、選択した行をダブルクリックします。「ユーザーの修正」ウィンドウが開きます。

➢ 「ユーザーの修正」ウィンドウで新しいユーザーの設定を行ってください。

➢ 設定が終わったら［OK］をクリックして確定します。

ユーザーの設定変更

- 「*iRMC* ユーザー管理」ダイアログボックスからユーザーを選択します。
- ［修正］ボタンをクリックし、選択したユーザーをダブルクリックします。「ユーザーの修正」ウィンドウが開き、選択されたユーザーの設定を表示します。
- 「ユーザーの修正」ウィンドウでこのユーザーの設定変更を行ってください。
- 設定が終わったら［*OK*］をクリックして確定します。

ユーザーの削除

- 「*iRMC* ユーザー管理」ダイアログボックスからユーザーを選択します。
- ［削除］ボタンをクリックしてユーザーを削除してください。

4.3.3 RMC S2 ユーザーの SSHv2 公開鍵認証

ユーザー名とパスワードによる認証方法に加えて、iRMC S2 は SSHv2 に基づくローカルユーザーの公開鍵と秘密鍵のペアを使用する公開鍵認証もサポートしています。SSHv2 公開鍵認証を実装するには、iRMC S2 ユーザーの SSHv2 鍵を iRMC S2 にアップロードし、iRMC S2 ユーザーはこのプログラム上でその秘密鍵を使用します。たとえば、PuTTY または OpenSSH クライアントプログラム の「ssh」などを使用します。

iRMC S2 は以下の種類の公開鍵をサポートしています。

– SSH DSS （最低条件）
– SSH RSA （推奨）

iRMC S2 にアップロードする公開 SSHv2 鍵は、RFC4716 フォーマットでも OpenSSH フォーマットでも使用可能です。(76 ページを参照してください。)

公開鍵認証

iRMC S2 の公開鍵認証は、おおむね以下のように処理されます。

iRMC S2 にログインしたいユーザーは鍵のペアを作成します。

– 秘密鍵は読み取り保護され、ユーザーのコンピュータ内に保存されます。

– ユーザー（または管理者）は、iRMC S2 に公開鍵をアップロードします。

設定が正しければ、ユーザーはパスワードの入力をしなくても非常に安全に、iRMC S2 にログインすることができるようになります。ユーザーの責任は秘密鍵の機密保護のみです。

秘密鍵の認証には以下の手続きが必要です。この手続きはこれ以降の節にも説明があります。

1. 「PuTTYgen」または「ssh-keygen」プログラムを使用して SSHv2 の公開鍵と秘密鍵を作成して、別々のファイルに保存します。(64 ページを参照してください。)
2. ファイルから SSHv2 鍵を iRMC S2 にアップロードします。(68 ページを参照してください。)
3. PuTTY または「ssh」プログラムを iRMC S2 の SSHv2 アクセス用に設定します。(70 ページ参照。)

PuTTY プログラムはフリーの SSHv2 鍵作成ツールです。インターネットから別途ダウンロードして下さい。ssh-keygen は OpenSSH で提供されるツールです。OpenSSH を別途ダウンロードしてください。
尚、PuTTY プログラム /ssh-keygen は参考（推奨）として記載しています。PuTTY プログラム／ssh-keygen のインストール、及び仕様、設定に関する質問、お問い合わせはご遠慮願います。

4.3.3.1 SSHv2 の公開鍵と秘密鍵の作成

SSHv2 の公開鍵と秘密鍵は以下のように作成することができます。

– プログラム *PuTTYgen* を使用する。または、

– OpenSSH クライアントプログラム、「ssh-keygen」を使用する

PuTTYgen を使用する SSHv2 の公開鍵と秘密鍵の作成
以下の通り進めます。

➤ ユーザーの Windows 機で *PuTTYgen* を起動します。

PuTTYgen が起動すると以下の画面が表示されます。

図 15： PuTTYgen：SSHv2 の新しい公開鍵と秘密鍵の作成

➤「Parameters」の項目で SSH-2RSA 鍵タイプを選択し［Generate］をクリックすると鍵の生成が開始されます。

鍵生成の進行状況は「Key」のペインに表示されます。（65 ページの図 16 を参照してください。）

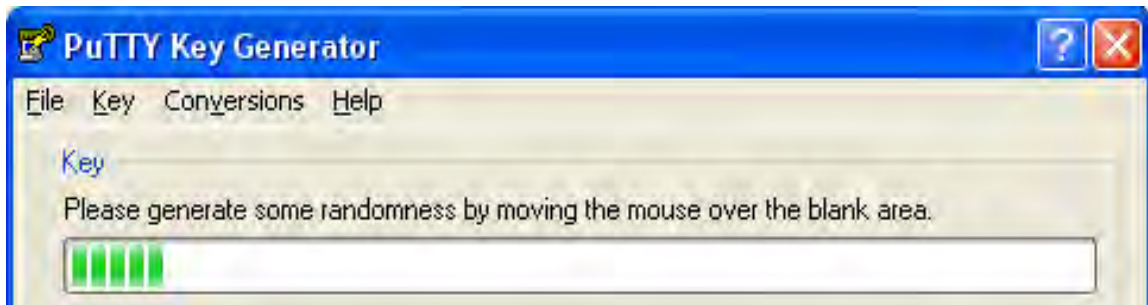



図 16： PuTTYgen： 新しい鍵のペアの作成（プログレスバー)

- ➢ 進行表示部の空白部分でマウスポインタを動かすと、作成される鍵のランダム性がより増加されます。

鍵が生成されると PuTTYgen が公開 SSHv2 鍵の指紋を表示します。

図 17： PuTTYgen、新しい SSHv2 鍵の作成（プログレスバー)

- ➢ ［Save public key］ボタンをクリックして、SSHv2 鍵をファイルに書き込んでください。このファイルから iRMC S2 に公開鍵をアップロードすることができます。(68 ページを参照してください。)

- ➢ ［Save private key］をクリックして、PuTTY に使用する秘密 SSHv2 鍵をセーブします。(70 ページ参照してください

ssh-keygen を使用する **SSHv2** の公開鍵と秘密鍵の作成

使用する Linux の版にプリインストールされていない場合には、
http://www.openssh.org から OpenSSH を入手できます。
OpenSSH 用オペランドの詳しい説明は http://www.openssh.org/manual.html 上の OpenSSH ユーザーガイドにあります。

以下の通り進めます。

➢ 「ssh-keygen」を呼び出して RSA 鍵のペアを生成させます。

ssh-keygen -t rsa

ssh-keygen は鍵生成処理の進行のログを作成します。「ssh-keygen」はユーザーに秘密鍵を保存するファイル名と秘密鍵のパスフレーズを問い合わせます。「ssh-keygen」は生成された SSHv2 の秘密鍵と公開鍵を別々のファイルに保存し、公開鍵の指紋を表示します。

例：「ssh -keygen」による RSA 鍵ペアの生成

解説：

1. 「*ssh-keygen*」は SSHv2 鍵をセーブするファイル名を要求します。［*Enter*］が押下されてファイル名なしの入力が確認されると「*ssh-keygen*」はデフォルト名の「*id_rsa*」を使用します。

2. 「*ssh-keygen*」から秘密鍵の暗号化に使用するパスフレーズの入力（および確認）が要求されます。［*Enter*］が押下されてパスフレーズなしの入力が確認されると、「*ssh-keygen*」はパスフレーズを使用しません。

3. 「*ssh-keygen*」は、新しく生成された秘密 SSHv2 鍵が「*/.ssh/id_rsa*」ファイルにセーブされたことを知らせます。

4. 「*ssh-keygen*」は、新しく生成された公開 SSHv2 鍵が「*/.ssh/id_rsa.pub*」ファイルにセーブされたことを知らせます。

5. 「*ssh-keygen*」は公開 SSHv2 鍵の指紋と公開鍵が属するローカルのログインを表示します。

4.3.3.2 SSHv2 鍵のファイルから iRMC S2 へのロード

以下の通り進めます。

➢ iRMC S2 の Web インターフェースから、iRMC S2 ユーザー管理ページの要求される一覧画面の詳細なビュー（この例では *user3*）を開きます。

図 18： iRMC S2 Web インターフェース 公開 SSHv2 鍵の iRMC S2 へのロード

➢ 「ファイルからのユーザー SSHv2 公開鍵アップロード」グループの中の［参照］ボタン (1) をクリックして、必要な公開鍵 (2) のあるファイルまで進みます。

➢ ［アップロード］ボタンをクリックして公開鍵を iRMC S2 にロードします。

鍵が正常にアップロードされると、iRMC S2 は「ファイルからのユーザー SSHv2 公開鍵アップロード」グループの中に Fingerprint を表示します。

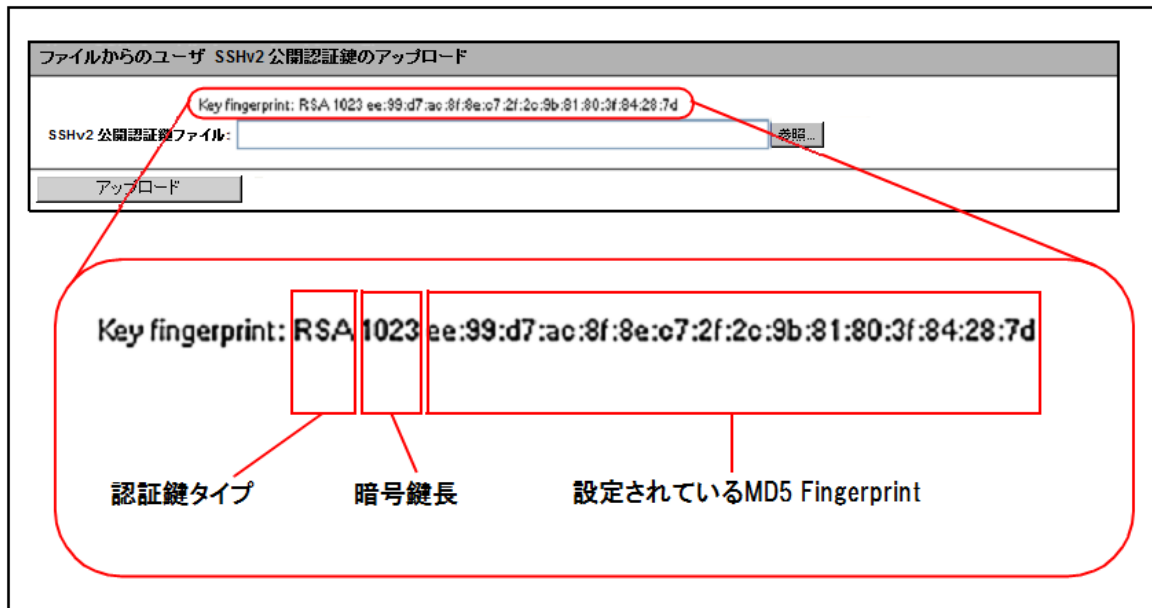



図 19： 鍵指紋の表示

i セキュリティのため、ここに表示された Fingerprint が PuTTYgen（65 ページの 図 17 を参照してください）や ssh-keygen（68 ページの例⑤を参照してください）に表示された Fingerprint と一致していることを確認してください。

4.3.3.3 PuTTY と OpenSSH クライアントが公開 SSHv2 鍵を使用するための設定

公開 SSHv2 鍵を使用する PuTTY の設定

PuTTY プログラムでは、iRMC S2 への接続の設定と、自身のユーザー名または自動ログイン機能によるログインが可能になります。PuTTY は、事前に生成された公開／秘密 SSHv2 鍵のペアに基づいて、自動的に認証プロトコルを処理します。

以下の通り進めます。

➢ ユーザーの Windows 機で PuTTY を起動します。
PuTTY が起動すると以下の画面が表示されます。

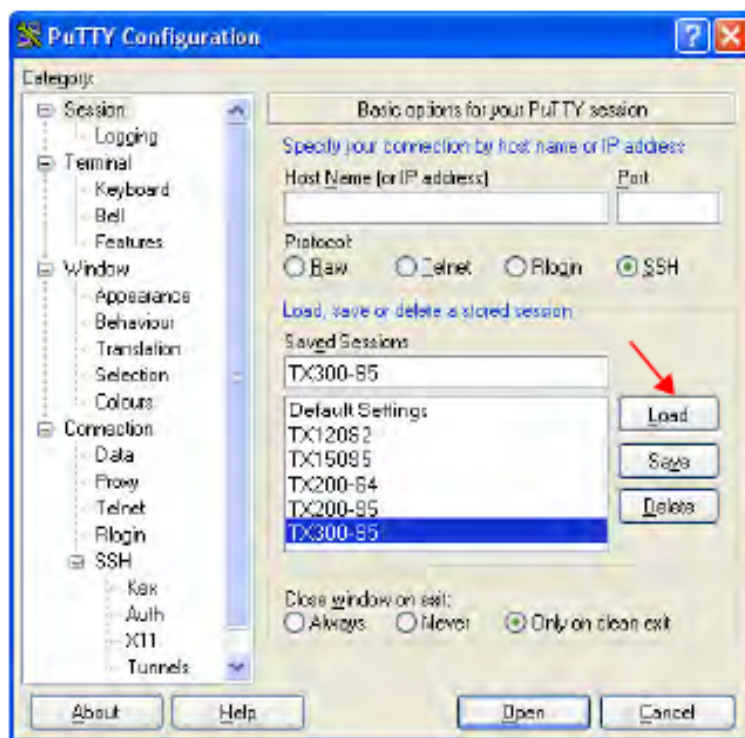



図 20： PuTTY：SSH セッションの選択とロード

➢ SSHv2 鍵を使用したい iRMC S2 に､セーブされた SSH セッションを選択するか新しい SSH セッションを作成します。

➢ ［Load］をクリックして選択した SSH セッションをロードします。その結果以下のウィンドウが開かれます。

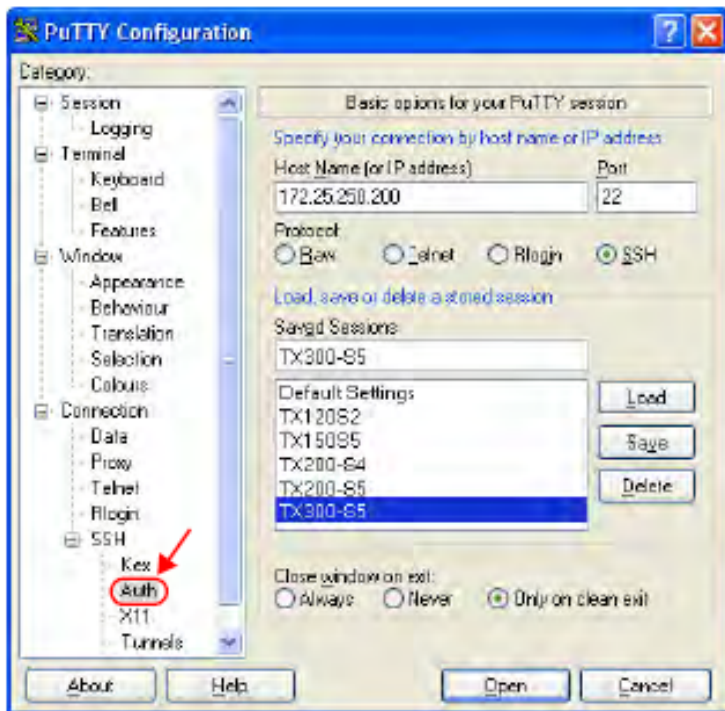



図 21： PuTTY：SSH セッションのロード

➢ SSH - Auth」を選択して、SSH 認証のオプションを設定します。
次に以下のウィンドウが開きます。（72 ページの図 22 を参照してください。）

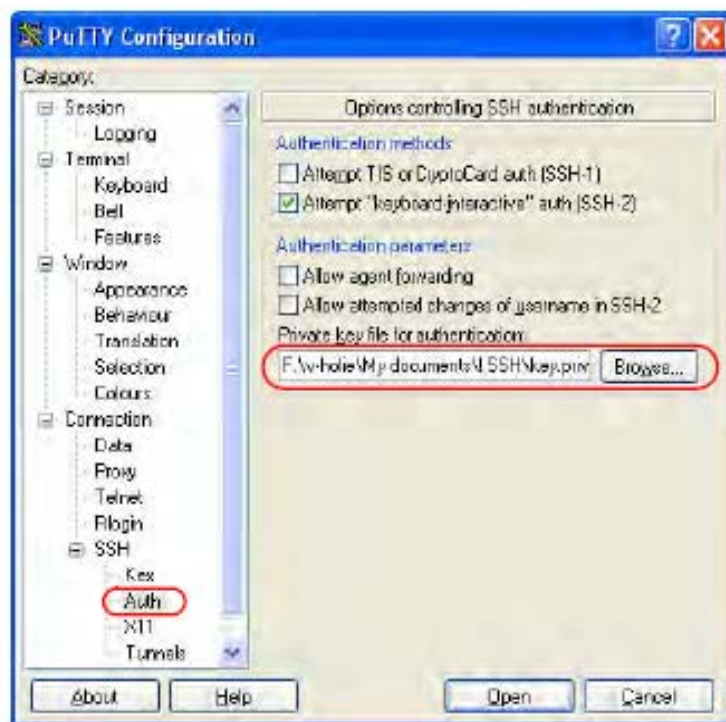



図 22： SSH 認証のオプションの設定

➢ iRMC S2 で使用したい秘密鍵が入ったファイルを選択します。

注意！

この時点では必要なのは秘密鍵（65 ページ参照）であり、iRMC S2 にロードされた公開鍵ではありません。

「Connection - Data」の下で、iRMC S2 に自動ログインするユーザー名を追加指定できます。

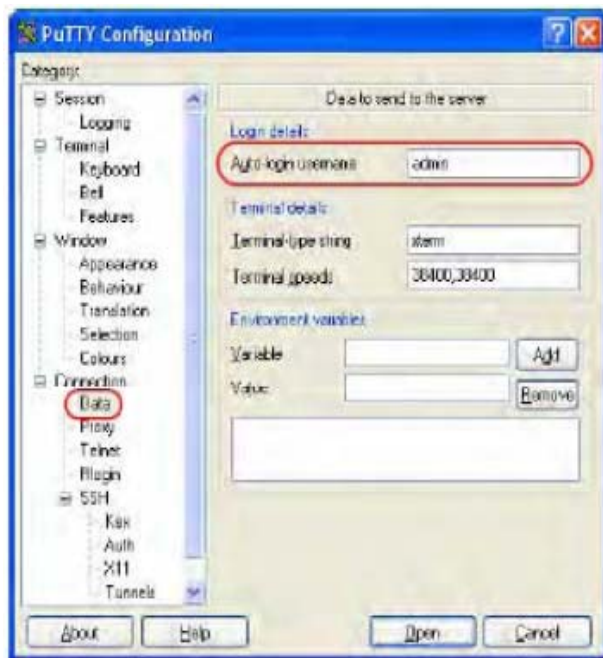



図 23： PuTTY：iRMC S2 に自動ログインするユーザー名の指定

公開 **SSHv2** 鍵に使用する **OpenSSH** クライアントプログラム **ssh** の設定

OpenSSH クライアントプログラム「ssh」を使用して SSHv2 で保護された接続を確立します。現在のローカルのログインのまま、あるいは、別のログインのどちらかでログインすることができます。

ログインは、iRMC S2 上のローカルログインとして設定され、関連する SSHv2 鍵は、iRMC S2 にロードされていなければなりません。

「ssh」は以下のソースから順番に設定オプションを読み込みます。

1. 「ssh」を呼び出すときに使用したコマンドライン引数
2. ユーザー毎の設定ファイル（$HOME/.ssh/config）

   このファイルにはセキュリティ上重要な情報は含まれていませんが、オーナーに はリード／ライトの許可のみが与えられます。ほかのどのユーザーもアクセスが 拒否されます。

3. システム全体の設定ファイル（/etc/ssh/ssh_config）
   以下の場合には、このファイルに設定パラメータのデフォルト値が書き込まれます。
   – ユーザー毎の設定ファイルがない、または、
   – ユーザー毎の設定ファイルに関連するパラメータが指定されていない。

最初に取得された値が各々のオプションに適用されます。

「ssh」の設定とそのオペランドに関する詳細な情報は以下のサイトの OpenSSH のペー ジから得ることができます。

http://www.openssh.org/manual.html

以下の通り進めます。

➢ 「ssh」を起動して、SSHv2 認証により iRMC S2 にログインします。

ssh -l [<user>] <iRMC_S2>

または

ssh [<user>@]<iRMC_S2>
<user>

iRMC S2 ログインに使用したいユーザー名。<user> を指定しない場合は、ssh は、iRMC S2 にログインしようとしているローカルコンピュータ上のログインユーザー名をそのまま使用します。

<iRMC_S2>

ユーザーがログインしようとする iRMC S2 名または、iRMC S2 のアドレス。

例：iRMC S2 上の SSHv2 認証ログイン

「ssh-」コールには、66 ページの「例 ：「ssh -keygen」による RSA 鍵ペアの生成」で示された通り、「ssh-keygen」が公開／秘密 RSA 鍵のペアを生成したものと見なされます。また、公開鍵は、iRMC S2 ユーザーの「user4」のために、iRMC S2 にロードされています。（68 ページを参照してください。）

ユーザーは「$HOME/User1」の下で自身のローカルコンピュータから、ログインユーザー 「user4」を使用して以下のように「RX100_S52-iRMC」にログインすることができます。

ssh user4@RX100_S52-iRMC

4.3.3.4 公開 SSHv2 の鍵（例）

RFC4716 フォーマットと OpenSSH フォーマットの両方による同じ公開 SSHv2 鍵を以下に示します。

RFC4716 フォーマットの公開 SSHv2 鍵

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH フォーマットの公開 SSHv2 鍵

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx

v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar

JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+F

pGJ2iw== rsa-key-20090401
```

4.4 iRMC S2 のグローバルユーザー管理

iRMC S2 のグローバルユーザー ID は、LDAP ディレクトリサービスを利用して集中管理されます。iRMC S2 ユーザー管理では、現在次のディレクトリサービスがサポートされます。

– Microsoft® Active Directory
– Novell® eDirectory（未サポート）
– OpenLDAP この節では次の点に関して説明します。
– iRMC S2 のグローバルユーザー管理の概略
– LDAP ディレクトリサービスによる iRMC S2 グローバルユーザー管理の概念
– ディレクトリサービスによるグローバル iRMC S2 ユーザー管理の設定（ディレクトリサービス中で、iRMC / iRMC S2 に特化した許可構造の生成）– Microsoft Active Directory によるグローバル iRMC S2 ユーザー管理
– Novell eDirectory によるグローバル iRMC S2 ユーザー管理（未サポート）
– OpenLDAP によるグローバル iRMC S2 ユーザー管理

本節で説明される、ディレクトリサービスのためにユーザー実行する作業とは別に、グローバルユーザー管理には、iRMC S2 上でローカルの LDAP 設定を設定する必要があります以下のいずれかの方法でローカル LDAP を設定します。

– iRMC S2 Web インターフェースにて行う（321 ページを参照してください。）

– Server Configuration Manager を使用する（427 ページを参照してください。）ディレクトリサービスを使用するには専門の知識が必要となります。ディレクトリサービスを熟知した管理者にて設定してください。

4.4.1 概要

iRMC S2（および iRMC）のグローバルユーザー ID は、ディレクトリサービスのディレクトリにすべてのプラットフォームの分が集中保管されています。このことによって、集中サーバによるユーザー ID 管理が可能となります。ネットワーク上でこのサーバに接続できるすべての iRMC や iRMC S2 でユーザー ID を使用することができます。

その上、iRMC / iRMC S2 のディレクトリサービスを使用することにより、管理されたサーバのオペレーティングシステムに使用されるものと同じユーザー ID を iRMC / iRMC S2 にも使用することが可能となります。

> グローバルユーザー管理は現在 iRMC S2 の以下の機能ではサポートされていません。
>
> – IPMI-over-LAN 経由のログイン
>
> – SOL 経由のコンソールのリダイレクション

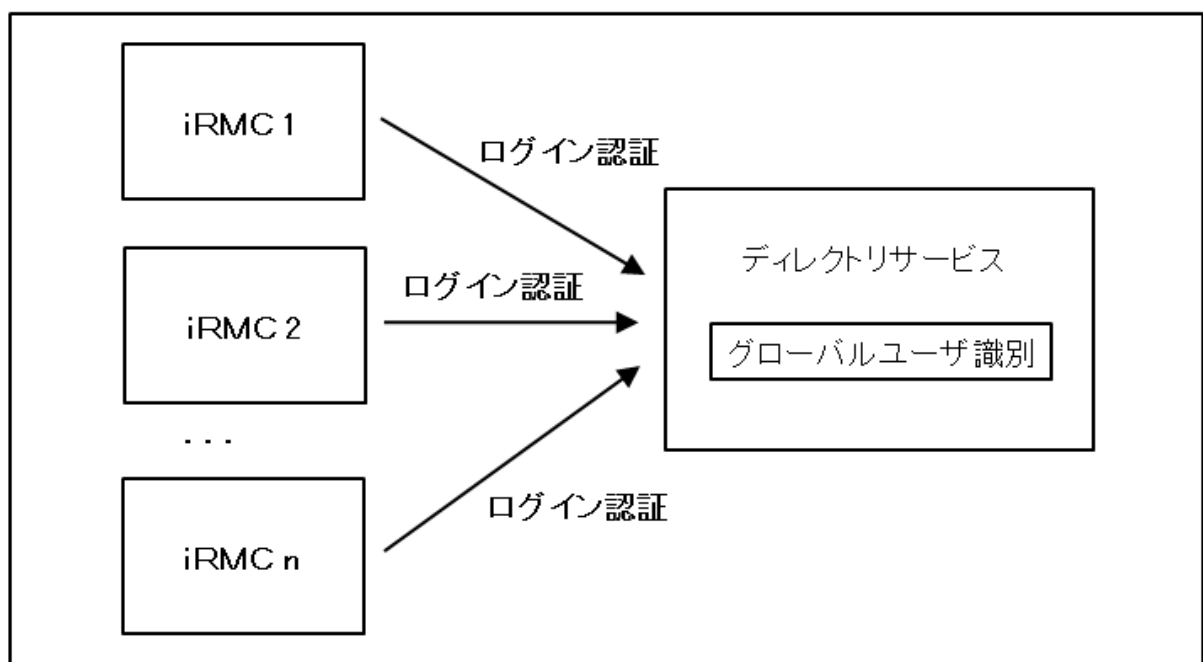



図 24： 複数の iRMC によるグローバルユーザー ID の共用

iRMCs ／ iRMC S2s と集中ディレクトリサービス間の通信はそれぞれ TCP/IP プロトコル LDAP （**L**ightweight **D**irectory **A**ccess **P**rotocol）経由で実行されます。LDAP によって、ディレクトリサービスにアクセスすることが可能となりますが、これは最もよく使われる方法であり、ユーザー管理には最も適しています。LDAP 経由の通信はオプションで SSL によるセキュリティ確保が可能です。

4.4.2 LDAP ディレクトリサービス経由の iRMC S2 のユーザー管理（概念）

以下に説明するディレクトリサービスに基づくグローバル iRMC S2 ユーザー管理の概念は、Microsoft Active Directory、および OpenLDAP に等しく適用されます。使用される図は、Microsoft Active Directory のユーザーインターフェース用の Active Directory Users and Computers コンソールの例に基づいています。

以下の記号は､LDAP 上で文字列を検索するためのメタキャラクタとして指定されています。*, \, &, (,), |, !, =, <, >, ~, :

したがって、ユーザーはこれらの記号を相対識別名（RDN）の要素として使用することはできません。

4.4.2.1 許可グループとロールを使用するグローバル iRMC S2 ユーザー管理

LDAP ディレクトリサーバ経由の iRMC ／ iRMC S2 グローバルユーザー管理には､標準のディレクトリサーバのスキーマを拡張する必要はありません。その代わりに、ディレクトリサーバ に関連するすべての情報は、ユーザーの許可（特権）も含めて、追加 LDAP グループと組織単位（OU）を経由して提供されます。これらの OU は、LDAP ディレクトリサーバのドメイン内の別々の OU が結合されたものです。（82 ページの図 26 を参照してください。）

– IRMC ユーザーは、組織単位（OU）｢iRMCgroups｣グループのメンバーになることにより特権を得ることができます。
– IRMC S2 ユーザーは、組織単位（OU）｢SVS｣で宣言されるロール（ユーザーロール）が割り当てられるか､または OU｢iRMCgroups｣のグループのメンバーとなることにより､特権を得ることができます。

OU「SVS」とストラクチャ「iRMCgroups」の両方がディレクトリサービスで定義されている場合には、ユーザーのログインデータはまず *SVS* のエントリと照合 され、ユーザー認証されます。一致するエントリが見つからない場合には、「iRMCgroups」のエントリとの一致を検索します。いずれの場合も最初に一致したエントリが適用されます。

ユーザーグループの許可直接割り当て

iRMC および iRMC S2（ファームウェアバージョン 3.77 以前）のグローバルユーザー管理では、許可の割り当てをユーザーグループにより管理します。この場合は、許可は個々のユーザーグループに直接割り当てられます。

ユーザーロール（略称 ロール）による許可の割り当て

iRMC S2（ファームウェアバージョン 3.77 以降）のグローバルユーザー管理では、許可の割り当てをユーザーロールにより管理します。この場合は、各ロールは、iRMC S2 上で有効なタスクに基づく許可プロファイルを個々に定義します。

各々のユーザーにはいくつかのロールが割り当てられますので、その結果、そのユーザーの許可は、割り当てられたロールすべての許可の合計により定義されます。

図 25 は Administrator、Maintenance、Observer および UserKVM の各ロールによるユーザー許可の、ロールに基づく割り当ての概念を図解したものです。

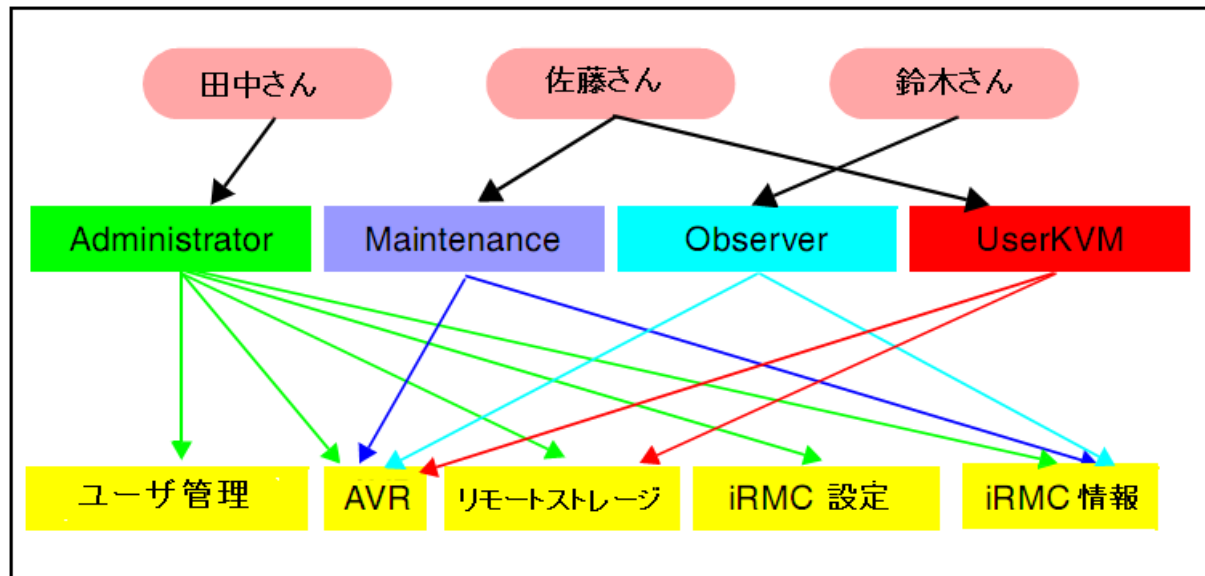



図 25： ユーザー許可のロールに基づく割り当て

ユーザーロールの概念には、以下のような重要な利点があります。

– 各々のユーザーまたはユーザーグループに、個別に許可を割り当てる必要がない。その代わりに、許可はユーザーロールに従って割り当てられる。

– 許可のストラクチャが変更になった場合にユーザーロールによる許可を適合させるのみでよい。

4.4.2.2 組織単位（**OU**）**SVS** と **iRMC** グループ

iRMC および iRMC S2 のファームウェアは現在 2 種類の LDAP ストラクチャをサポートしています。

– iRMC S2 、ファームウェアバージョン 3.77A まで
  LDAP v2 ストラクチャをサポートし、OU SVS に保存されています。
  LDAP v2 ストラクチャは将来的な機能拡張を考慮して導入されました。
– iRMC S2 のバージョン 3.77A 以前のファームウェアと iRMC
  LDAP v1 ストラクチャをサポートし、OU「 *iRMCgroups*」に保存されています

このため、以下のように推奨いたします。

– サーバーパックが iRMC S2 のみの PRIMERGY サーバで設定されている場合には、ディレクトリサーバのグローバルユーザー管理には、LDAP v2 ストラクチャのみを使用してください。この場合はすべての iRMC S2 に 3.77A 以降のバージョンがインストールされていることを確認してください。
– PRIMERGY サーバで、iRMC S2 と iRMC の両方が運用されている場合には、グローバルユーザー管理には、LDAP v1 ストラクチャと LDAP v2 ストラクチャの両方のディレクトリサーバが必要です。

> **i** ソフトウェアツール「SVS_LdapDeployer」（90 ページ参照）を使用して、LDAP v1 と LDAP v2 ストラクチャを生成し、並存する LDAP v1 と LDAP v2 ストラクチャを維持管理します。

iRMCgroups と SVS の OU のストラクチャは以下の通りです。

– 「*iRMCgroups*」には「*Departments*」と「Shell」の OU が含まれています。
  – 「*Departments*」にはユーザー特権のためのグループが含まれています。
  – 「*Shell*」にはユーザーシェルのためのグループが含まれています。
– SVS には「*Declarations*」、「*Departments*」および「*User Settings*」が含まれています。
– 「*Declarations*」には定義されたロールのリストと予め定義された iRMC S2 ユーザー許可のリストが含まれています。（56 ページ、「ユーザー権限」の節を参照してください。）
– 「*Departments*」にはユーザー特権のためのグループが含まれています。
– 「*User Settings*」には、メールのフォーマット（警告メールに使用します）などのユーザーまたはユーザーグループの個々の詳細と、ユーザーシェルのグループが含まれています。

たとえば、Microsoft Active Directory の場合には、iRMC S2 ユーザーのエントリは標準 OU の Users に納められています。ただし、iRMC S2 ユーザーは標準ユーザーとはことなり、「*SVS*」OU または「*iRMCgroups*」OU のひとつまたは複数のグループのメンバにもなっています。

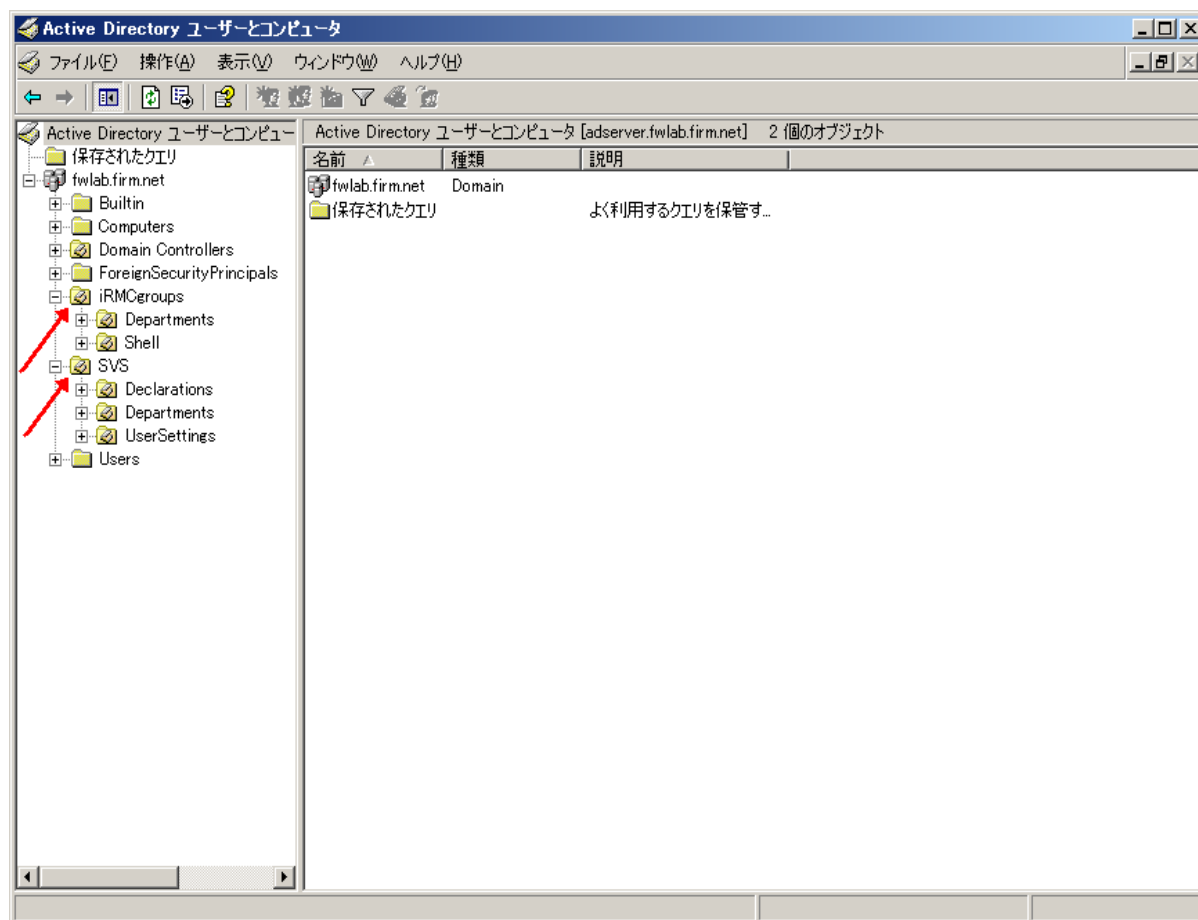



図 26 : 「SVS」と「iRMCgroups」OU は「fwlab.firm.net」のドメインにあります。

i バージョン 3.6x のファームウェアでは、iRMC S2 用のユーザーエントリは基本ドメインの配下のどのポイントにも配置できます。許可グループも基本ドメインの配下のどのポイントにも配置できます。

4.4.2.3 他部門サーバからのアクセス許可

大規模な企業では、iRMC S2 によって管理されるサーバ群は通常ことなる部署に割り当てられます。その上、管理対象サーバの管理者権限も、多くの場合部門独自の方法で割り当てられます。

部門は「**Departments**」という **OU** 内で結合されます

「Departments」OU は、iRMC S2 によって管理されるサーバを結合し、多数のグループを形成します。この方法は、同じユーザー ID と許可が適用される部門にも対応します。たとえば、84 ページの 図 27 では「DeptX」、「DeptY」および「Others」の各部門となります。

「Others」のエントリは随意ですが推奨します。「Others」はこれらのサーバすべてに内包される予め定義された部門名で、他の部門に属することはありません。「Departments」のは以下にリストされる部門（OU）の数に関しては、制限はありません。

iRMC S2 でディレクトリサービスを iRMC S2 Web インターフェース経由（321 ペー ジ参照）、Server Configuration Manager 経由（ 427 ページ参照）、または Server Management Tool（IPMIVIEW）経由で設定する場合には、関連する iRMC S2 を運用 する管理されたサーバが属する部門の名前を指定します。LDAP ディレクトリにその名 前の部門がない場合には、*Others* 部門にある許可を使用します。

84 ページの図 27 は、Active Directory ユーザーとコンピュータを基本とした、このタイプの組織構造の例を表します。

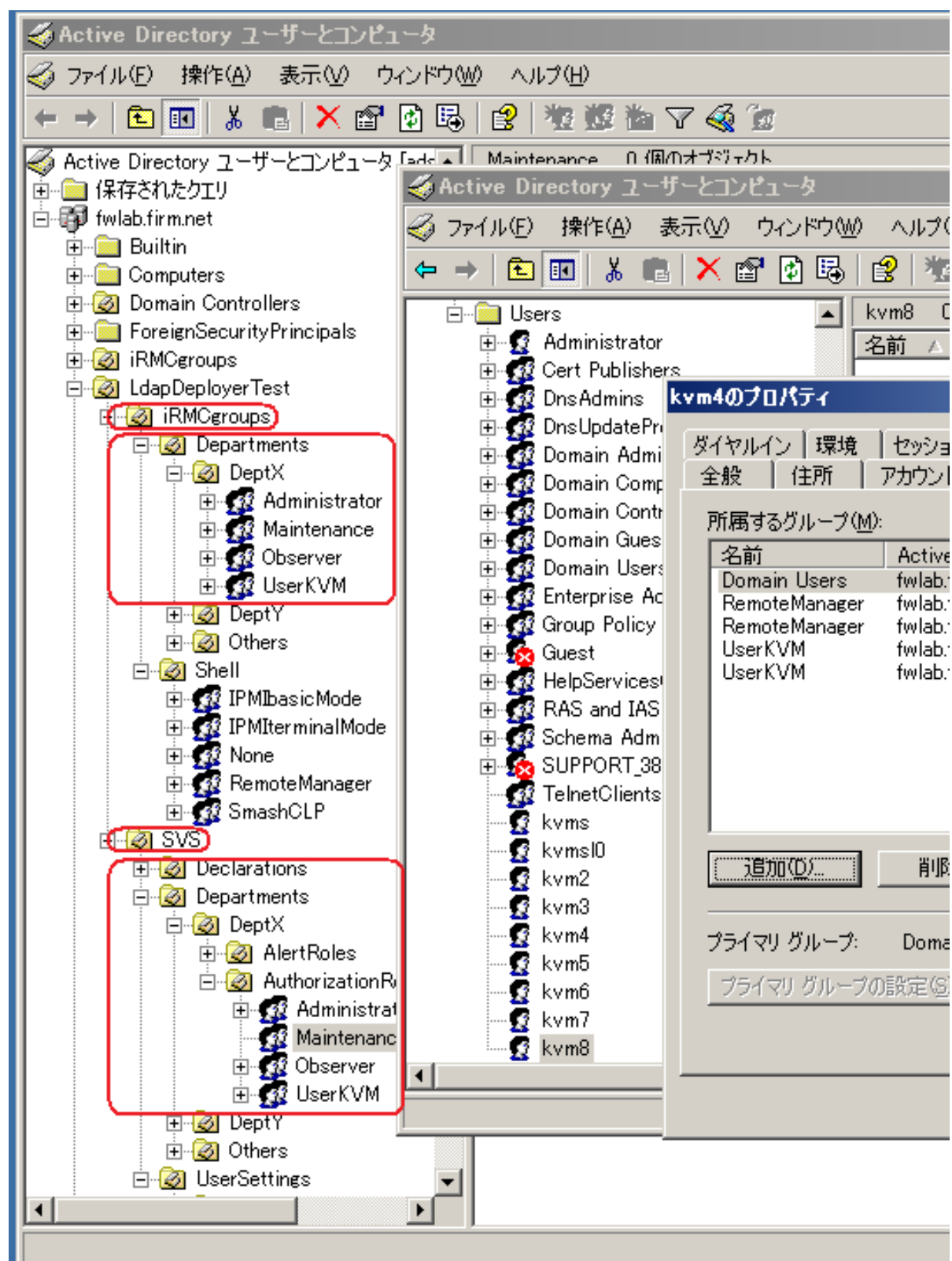



図 27： ドメイン「fwlab.firm.net」の組織構造

4.4.2.4 iRMCgroups 許可のプロファイルは許可グループ経由で定義されます

関連する許可グループ（セキュリティグループ）は各部門の直下にリストされます（84 ページの図 27)。許可グループの数に関しては、制限はありません。許可グループの名前は必要に応じて選ぶことがで きますが、運用するディレクトリサービスに賦課された特定の構文要件に合わなければなりません。各々の許可グループは特有のパーミッションプロファイルを定義しますが、それが関連する許可グループに所属するすべてのユーザーに適用されます。

注意！

同一部門内でユーザーが複数の許可グループに同時に所属することのないよう確認してください。（ユーザーが同一部門で複数の許可グループに所属している場合には、必 ず LDAP クエリから返される最初の結果が適用されます。）

グローバル iRMC S2 ユーザー管理には、チャンネル特有の許可グループも含まれます。（56 ページを参照してください。）個々のユーザー許可に関する詳細情報は、56 ページの「ユーザー権限」の節を参照してください。

たとえば、部門（DeptX など）をクリックした場合には、先ず Active Directory ユーザーとコンピュータの階層ツリー（86 ページの図 28 参照）の (1)、次に、この部門に定義された許可グループ（セキュリティグループ）が表示部にリストされます（この例では「DeptX」)。

表示されたセキュリティグループ (2) の中からひとつをクリックして、セキュリティグループ用の 「Properties」ダイアログを開くことができます（この例では「Maintenance」)。

関連する許可は以下のシンタックスにより「Notes」の下にリストされます。

注意！

「Notes」フィールドの下のユーザープロファイルを変更しないこと。変更するとログインできなくなります。ロールの変更には必ず SVS_LdapDeployer を使用します。（90 ペー ジを参照してください。）

LAN: OEM | Administrator | Operator | User | None

Serial: OEM | Administrator | Operator | User | None

UserAccounts: On | Off

iRMCsettings: On | Off

Video Redirection: On | Off

Remote Storage: On | Off

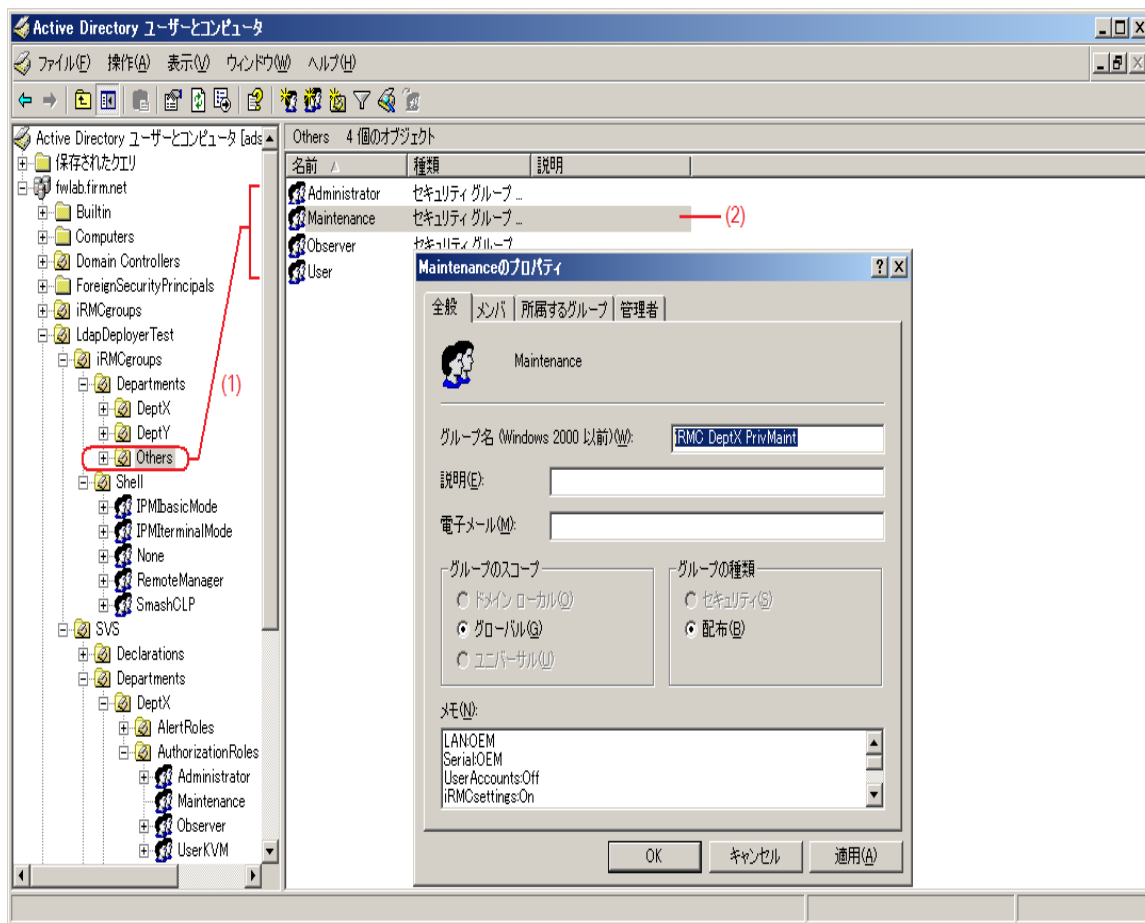



図 28： 「Maintenance」セキュリティグループのプロパティダイアログ

動作シェルの設定

LDAP サーバでは、ユーザークセス許可のみではなく、ユーザーの動作シェルも指定することができます。許可の割り当てとはことなり、動作シェルの定義は完全にユーザー特有であり、部門には依存しません。

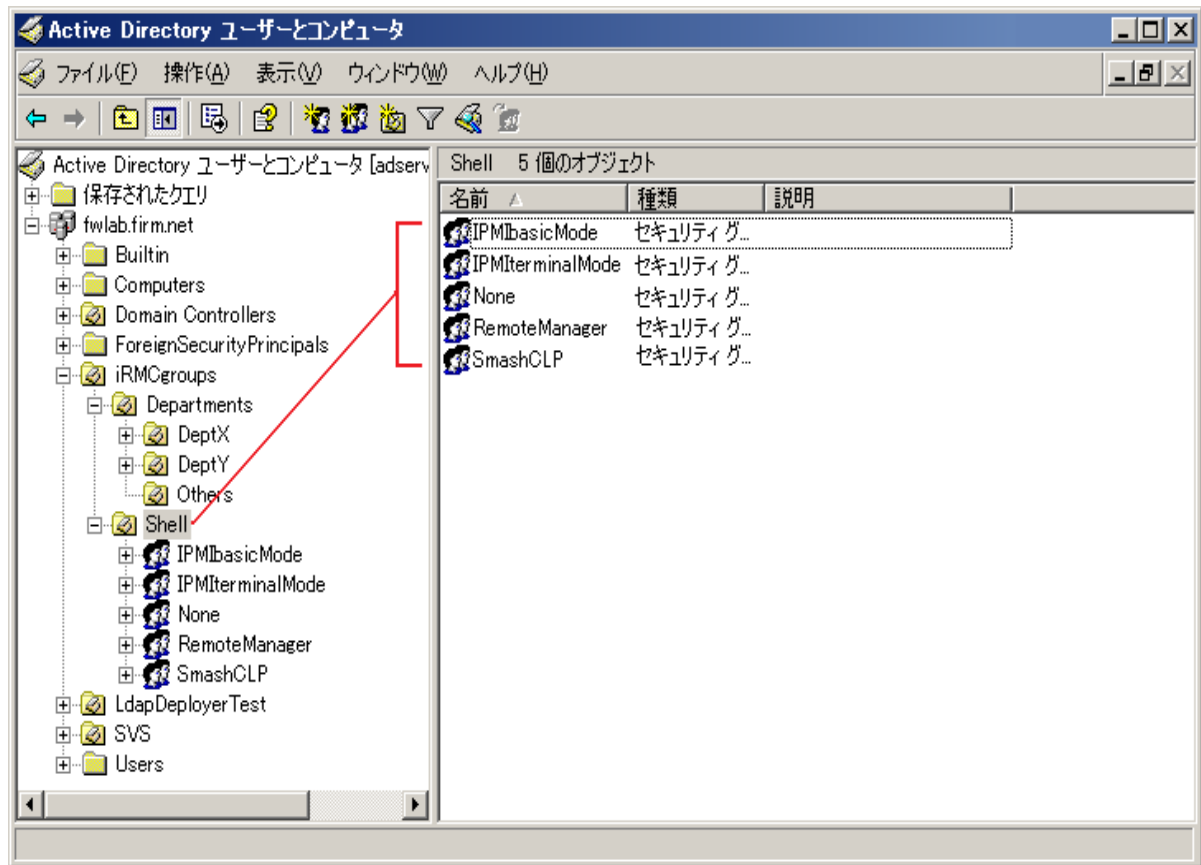



図 29： 動作シェルの定義

以下のグループを選択できます。

– 「*IPMIbasicMode*」
– 「*IPMIterminalMode*」
– 「*None*」
– 「*RemoteManager*」 （361 ページ参照）.
– 「*SmashCLP*」 （381 ページ参照）.

ユーザーは単一のシェルグループのみに所属できます。
複数のシェルグループに所属するユーザーは、自動的にそれらのグループの中で最も優先度が高いグループに割り当てられます。
優先度の順位は上記にリストされた通りです（優先度は上から下に行くにしたがって 低くなります）。
シェルグループに属さないユーザーはいずれもデフォルトとして「*Remote Manager*」グループに割り当てられます。

4.4.2.5 SVS: 許可のプロファイルはロール経由で定義されます

要求される関連ユーザーロール（認証ロール）は各部門の直下にリストされます（84 ページの図 27）。ここでリストされるロールはすべて「Declarations」OU で定義されます。それ以外にロールの数に 関する制限はありません。ロールの名前は必要に応じて選ぶことができますが、運用するディレクト リサービスに賦課された特定のシンタックス要件に合わなければなりません。各認証ロールは、iRMC S2 上の処理のためにタスクに基づく許可プロファイルを個々に定義します。

認証ロールと同様に警告ロールもリストされます。各々の警告ロールは Email で警告するために個々の警告プロファイルを定義しています。（145 ページ「グローバル iRMC S2 ユーザー宛の Email 警告の設定」の節を参照してください。）

ユーザーロールの表示

「Active Directory ユーザーとコンピュータ」ストラクチャツリー（図 30 参照）の「SVS」の配下にある（1）部門（たとえば「DeptX」）を選択し、関連するノード「DeptX – Authorization Roles」を展開すると、この部門に定義されたユーザーロール（ここでは「DeptX」）（2）が表示されます。

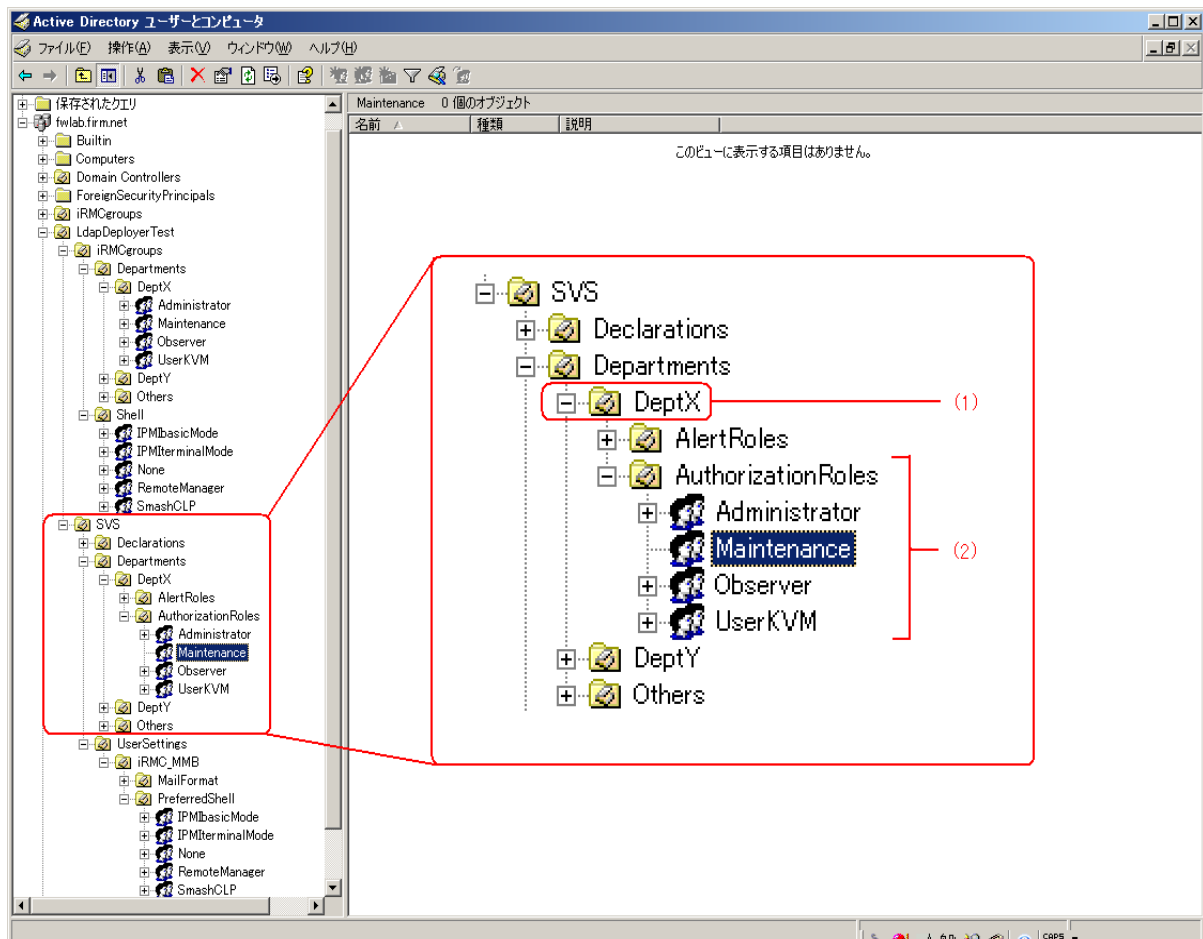



図 30 : 「ユーザーとコンピュータ」スナップインの中のユーザーロールの表示

ActiveDirectory 権限グループの表示

「Active Directory ユーザーとコンピュータ」ストラクチャツリー（図 31 参照）の「Users」の配下にある（1）ユーザー（たとえば「kvms4」）を選択し、コンテキストメニューから「プロパティ – メンバ」を選択してこのユーザーの「プロパティ」ダイアログボックスを開くと、ユーザーが所属する許可グループ（ここでは「kvms4」）が（2）「メンバ」タブの中に表示されます。

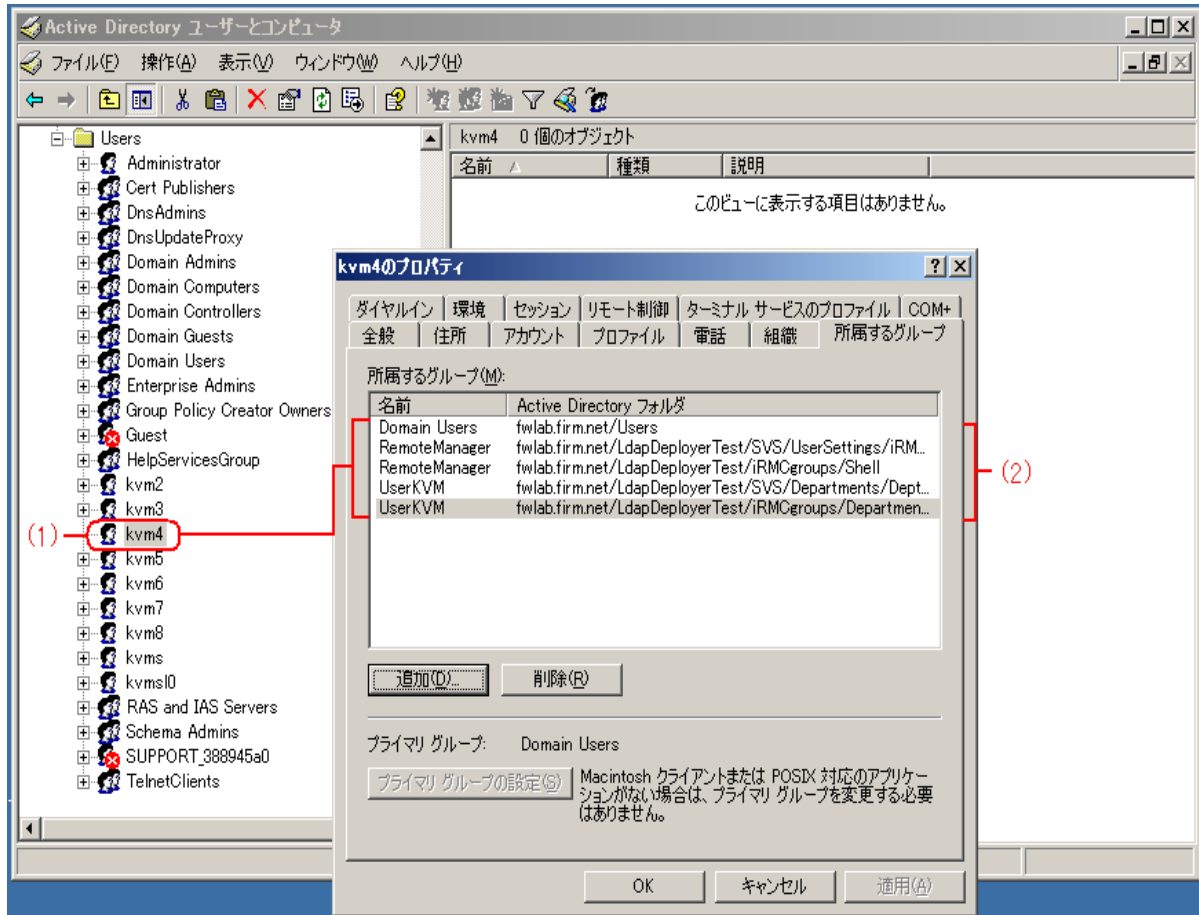



図 31：ユーザー「kvms4」のプロパティダイアログボックス

4.4.3 SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除

ディレクトリサービスを使用してグローバル iRMC S2 ユーザー管理を操作できるようにするために、LDAP ディレクトリサービスの中に「SVS」と「iRMCgroups」ストラクチャ（OU）を作成する必要があります。

「SVS」と「iRMCgroups」ストラクチャの生成または変更には「SVS_LdapDeployer」を使用してください。「SVS_LdapDeployer」は Java アーカイブ（「SVS_LdapDeployer.jar」）ですが、ServerView Suite の DVD 1 の中で提供されています。

この節では以下を説明いたします。

– 「SVS_LdapDeployer」の設定ファイル

– 「SVS_LdapDeployer」

– 「SVS_LdapDeployer」のコマンドとオプション

– 通常の使用例

4.4.3.1 設定ファイル（XML ファイル）

「SVS_LdapDeployer」は XML 設定ファイルに基づいて、LDAP ストラクチャを生成します。この入力ファイルには *SVS* あるいは「iRMCgroups」ストラクチャの XML 構文によるストラクチャ情報が含まれています。

設定ファイルの構文はサンプル設定ファイル、「Generic_Settings.xml」および「Generic_InitialDeploy.xml」によって開設されます。サンプルファイルは ServerView Suite の DVD1 の中の jar アーカイブ、「SVS_LdapDeployer.jar」にあります。

ディレクトリサーバ接続のための有効な接続データはかならず <Settings> 入力ファイルの下に入力しなければなりません。

サーバにアクセスするための認証データは任意で入力することができます。その代わりに、認証データを「SVS_LdapDeloyer」のコマンドラインの中に指定することもできます。

認証データを設定ファイルまたはコマンドラインに指定しなかった場合には、「SVS_LdapDeployer」を呼び出す際に「SVS_LdapDeployer」から認証データをランタイムで入力するように督促されます。

4.4.3.2 SVS_LdapDeployer の起動

「SVS_LdapDeployer」は以下の手順で起動してください。

- Java アーカイブ（「jar archive」）の「SVS_LdapDeployer.jar」をディレクトリサーバのフォルダにセーブします。
- ディレクトリサーバのコマンドインターフェースを開きます。
- 「jar」アーカイブ、「SVS_LdapDeployer.jar」が保存されているフォルダに移動します。
- 次の構文を使って「SVS_LdapDeployer」を呼び出します。

java -jar SVS_LdapDeployer.jar <command> <file>
[<option>...]

「SVS_LdapDeployer」が稼働中に処理するさまざまな手順の情報を見ることができます。詳細な情報は「log.txt」ファイルから見ることができます。このファイルは 「SVS_LdapDeployer」稼働時に毎回実行フォルダの中に作られます。

<command>

実行する処理を指定します。
以下のコマンドを使用可能です。

-deploy

グローバル iRMC / iRMC S2 ユーザー管理の LDAP ストラクチャをディレクトリサーバの中に作成します（93 ページを参照してください）

-delete

グローバル iRMC / iRMC S2 ユーザー管理に使用した LDAP ストラクチャをディレクトリサーバから削除します（95 ページを参照してください）。

-import

既存の LDAP v1 ストラクチャから 同等の LDAP v2 ストラクチャを作成します（93 ページを参照してください）

-synchronize

LDAP v2 になんらかの変更がある場合、既存の LDAP v1 ストラクチャを同じように変更します（93 ページを参照してください）。

<file>

「SVS_LdapDeploy」が入力ファイルとして使用する設定ファイル（「.xml」）です。この設定ファイルには、ストラクチャ「SVS」もしくは「iRMCgroups」の「XML」構文によるストラクチャ情報が含まれています。

設定ファイルの構文は、サンプル設定ファイル、「Generic_Settings.xml」および「Generic_InitialDeploy.xml」で解説されます。これらのファイルは「 jar」アーカイブ、「SVS_LdapDeployer.jar」と一緒に、ServerView Suite の DVD 1 の中に入っています。

<option> [<option> ...]

指定されたコマンドの実行をコントロールするためのオプションです。

これ以降の節では「SVS_LdapDeployer」で使用できる個々のコマンドの詳細と、関連するオプションと合わせて解説します。

「SVS_LdapDeployer」は、すべてのグループが含まれるサブツリーを生成しますが、ユーザーとグループの関連付けはしません。ユーザーエントリは、OU「SVS」もしくは「iRMCgroups」がディレクトリサービス の中に生成された後、運用するディレクトリサービスの適切なツールを使用して作成し、割り当てます。

4.4.3.3 -deploy（展開）: LDAP ストラクチャの作成と変更

「-deploy」コマンドを使用して、ディレクトリサーバ上に新し、LDAP ストラクチャを作成したり、既存の LDAP ストラクチャに新しいエントリを追加したりことができます。

既存の LDAP ストラクチャからエントリを削除する場合は、先ず「-delete」(95 ペー ジ参照) を使用して、LDAP ストラクチャ自体を削除し、次に適切に選んだ設定ファイルを使用して再作成します。

構文 :

```
-deploy <file> [-structure {v1 | v2 | both}]
        [ -username <user>]
        [ -password <password>][ -store_pwd <path>][ -kloc <path>]
        [ -kpwd [<key-password>]]
```

<file>

設定データを含む *XML* ファイル。

設定ファイルの <Data> 部にはストラクチャを最初に生成するため、または展開するために必要なロールと部門がすべて含まれなければなりません。

-structure v1 | -structure v2 | -structure both
LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを作成します。

-username <user>
ディレクトリサーバにログインするためのユーザー名。

-password <password>
ユーザー <user> のパスワード。

-store_pwd

「-deploy」が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルに暗号化されたパスワードをセーブします。初期設定では、ランダムに生成された鍵は「SVS_LdapDeployer」が実行されるフォルダに保存されます。

注意！

ランダムに生成された鍵は安全な場所にセーブしてください。予め定義されたターゲットフォルダがセキュリティの面で適切でない場合、または他のユーザーも鍵がセーブされたフォルダにアクセスできる場合は、「-kloc」と「-kpwd」オプションを使用して、鍵を安全にセーブしてください。

-kloc <path>

ランダムに生成された鍵を <path> の下にセーブします。
このオプションが指定されない場合には、鍵は「SVS_LdapDeployer」が実行されるフォルダにセーブされます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。
<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。

4.4.3.4 -delete: LDAP ストラクチャの削除

「-delete」コマンドを使用して、ディレクトリサーバから LDAP ストラクチャを削除できます。

構文：

-deploy <file> [-structure {v1 | v2 | both}]
[-username <user>]
[-password <password>][-store_pwd <path>][-kloc <path>]
[-kpwd [<key-password>]]

<file>
削除するストラクチャを指定する *XML* ファイルです。

-structure v1 | -structure v2 | -structure both
LDAP v1 ストラクチャまたは、LDAP v2 ストラクチャ、あるいは、LDAP v1 と LDAP v2 両方のストラクチャを削除します。

-username <user>
ディレクトリサーバにログインするためのユーザー名です。

-password <password>
ユーザー <user> のパスワード。

-stor_pwd
-delete が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルに暗号化されたパスワードをセーブします。初期設定では、ランダムに生成された鍵は「SVS_LdapDeployer」が実行されるフォルダに保存されます。

注意！

ランダムに生成された鍵は安全な場所にセーブしてください。予め定義されたターゲットフォルダがセキュリティの面で適切でない場合、または他のユーザーも鍵がセーブされたフォルダにアクセスできる場合は、「-kloc」と「-kpwd」オプションを使用して、鍵を安全にセーブしてください。

-kloc <path>
ランダムに生成された鍵を <path> の下にセーブします。
このオプションが指定されない場合には、鍵は *SVS_LdapDeployer* が実行されるフォルダにセーブされます。

-kpwd [<password>]
ランダムに生成された鍵を保護するためのパスワードを指定します。
<password> が指定されない場合は、現行のランタイムのスナップショットを元にしてパスワードが自動的に生成されます。

4.4.3.5 -import: LDAP v1 ストラクチャを LDAP v2 ストラクチャにインポートします

-import コマンドを使用すると､既存の LDAP v1 ストラクチャから同等の LDAP v2 ストラクチャを、ディレクトリサーバ上に生成させることができます。

構文：

```
-import <file>[ -username <user>]
        [ -password <password>][ -store_pwd <path>][ -kloc <path>]
        [ -kpwd [<key-password>]]
```

<file>

インポートするストラクチャを指定する *XML* ファイルです。

-username <user>

ディレクトリサーバにログインするためのユーザー名です。

-password <password>

ユーザー <user> のパスワード。

-stor_pwd

-import が正常に実行された後に、パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルに暗号化されたパスワードをセーブします。初期設定では、ランダムに生成された鍵は「SVS_LdapDeployer」が実行されるフォル ダに保存されます。

注意！

ランダムに生成された鍵は安全な場所にセーブしてください。予め定義されたターゲットフォルダがセキュリティの面で適切でない場合、または他 のユーザーも鍵がセーブされたフォルダにアクセスできる場合は､「-kloc」と「-kpwd」オプションを使用して鍵を安全にセーブしてください。

-kloc <path>

ランダムに生成された鍵を <path> の下にセーブします。

このオプションが指定されない場合には、鍵は「SVS_LdapDeployer」が実行されるフォルダにセーブされます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。

<password> が指定されない場合は、現行のランタイムのスナップショットを基にしてパスワードが自動的に生成されます。

4.4.3.6 -synchronize: LDAP v2 ストラクチャに行った変更を、LDAP v １ ストラクチャ上で同期して変更します

LDAP v1 と LDAP v2 ストラクチャが混在する設定では、「-synchronize」コマンドを使用すると LDAP v2 上で行った変更を既存の LDAP v1 ストラクチャに同期させて変更することができます。

変更は必ず LDAP v2 ストラクチャ上で行ってください！

構文：

-import <file>[-username <user>]
[-password <password>][-store_pwd <path>][-kloc <path>]
[-kpwd [<key-password>]]

<file>

インポートするストラクチャを指定する XML ファイルです。

-username <user>

ディレクトリサーバにログインするためのユーザー名。

-password <password>

ユーザー <user> のパスワード。

-stor_pwd

-synchronize が正常に実行された後に､パスワード <password> をランダムに生成された鍵を使用して暗号化し、設定ファイルに暗号化されたパスワードをセーブします。初期設定では、ランダムに生成された鍵は「SVS_LdapDeployer」が実行されるフォルダに保存されます。

注意！
ランダムに生成された鍵は安全な場所にセーブしてください。予め定義されたターゲットフォルダがセキュリティの面で適切でない場合、または他 のユーザーも鍵がセーブされたフォルダにアクセスできる場合は、「-kloc」と「-kpwd」オプションを使用して鍵を安全にセーブしてください。

-kloc <path>

ランダムに生成された鍵を <path> の下にセーブします。
このオプションが指定されない場合には、鍵は「SVS_LdapDeployer」が実行されるフォルダにセーブされます。

-kpwd [<password>]

ランダムに生成された鍵を保護するためのパスワードを指定します。
<password> が指定されない場合は、現行のランタイムのスナップショットを元にしてパスワードが自動的に生成されます。

4.4.4 一般的な使用例

「SVS_LdapDeployer」を使用する際の一般的な使用例は以下に述べるとおりです。

4.4.4.1 LDAP v1 と LDAP v2 ストラクチャを並存させる初期設定の実施

iRMC と、iRMC S2 のグローバルユーザー管理を初めて設定する場合、これを行うために LDAP v1 と LDAP v2 の両方のストラクチャが必要となります。

推奨する方法。

1. LDAP v1 と LDAP v2 ストラクチャの部門定義を生成します。

   (「iRMCgroups」および「SVS」):

   java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
   -structure both

2. 今後行われる変更は、LDAP v2 ストラクチャ上のみで行い、「- synchronize」コマンドを使用して、LDAP v1 ストラクチャに転送します。(97 ページを参照してください。)。

   java -jar SVS_LdapDeployer.jar -synchronize mySettings.xml

4.4.4.2 LDAP v1 ストラクチャの LDAP v2 へのインポート

LDAP v1 に基づく iRMC と、iRMC S2 のグローバルユーザー管理をすでに運用しており、今後 LDAP v2 も運用したい場合

推奨する方法。

1. 既存の LDAP v1 ストラクチャ(「iRMCgroups」)を LDAP v2 ストラクチャ(「SVS」)にインポート(変換)します。両方のストラクチャは並存します。

   java -jar SVS_LdapDeployer.jar -import mySettings.xml

   このステートメントにより、部門の定義とユーザーの許可グループへの割り当ては、既存の LDAP v1 ストラクチャから新し、LDAP v2 ストラクチャにコピーされます。

2. 今後行われる変更は、LDAP v2 ストラクチャ上のみで行い、「- synchronize」コマンドを使用して、LDAP v1 ストラクチャに転送します。(97 ページを参照してください。)。

   java -jar SVS_LdapDeployer.jar -synchronize mySettings.xml

4.4.4.3 LDAP v2 ストラクチャの再生成と展開

LDAP v2 ストラクチャ を再生成、または展開したい場合推奨する方法。

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
    -structure -structure v2
```

または

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
```

4.4.4.4 LDAP v2 ストラクチャの再生成と認証データの督促およびセーブ

LDAP v2 ストラクチャを再生成したい場合
認証データはコマンドラインを使用して作成しセーブされます。

推奨する方法。

```
java -jar SVS_LdapDeployer.jar -deploy myInitialDeploy.xml
        -store_pwd -username admin -password admin
```

ログインデータをセーブした後、「SVS_LdapDeployer」を使用してユーザー名およびとパスワードを指定せずにディレクトリサーバに接続してください。使用可能な数値が XML 設定ファイルに穂陣されている場合には「SVS_LdapDeployer」はその数値を 使用します。「SVS_LdapDeployer」はパスワードが暗号化できれば、セーブされたパスワードのみを使用します。そのため、前回のコールで適用したものと同じランタイ ム環境で「SVS_LdapDeployer」を「-store_pwd」と一緒に実行する必要があります。 （94 ページを参照してください。）このコンテキストの中の「同じランタイム環境」とは、「同じコンピュータを使用する同じユーザー」または「鍵が保存されたフォルダにアクセスする許可を持つユーザー（「-kloc」オプション、94 ページ参照）」を意味します。

今後は、「SVS_LdapDeployer」を呼び出した際にすでにセーブされたユーザーカウントを使用することもできます。さらに、データをコマンドラインに明確に指定するか、「SVS_LdapDeployer」がそのように要求する場合には、他の認証データも一時的に使用することができます。

4.4.5 Microsoft Active Directory による iRMC S2 ユーザー管理

本節は、iRMC S2 ユーザー管理を Microsoft Active Directory に統合する方法を説明します。

前提条件：

LDAP v1 もしくは、LDAP v2 ストラクチャが Active Directory サービスの中に生成されていること。（97 ページ、「SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除」の節を参照してください。）

以下の手順を実行して、iRMC S2 ユーザー管理を Microsoft Active Directory に統合します。

1. iRMC S2 のユーザーを Active Directory の iRMC S2 ユーザーグループに割り当てます。
2. Active Directory サーバ上で、iRMC S2 LDAP/SSL アクセスを設定します。

4.4.5.1 Active Directory サーバ上の iRMC S2 LDAP/SSL アクセスの設定

> **i** iRMC S2-LDAP の統合には、OpenSSL プロジェクトに基づき、Eric Young 氏が開発した SSL 実装を使用します。SSL copyright の複製リストを 153 ページに掲載します。

iRMC S2 が SSL 経由で LDAP を使えるようにするには RSA の証明書が必要です。
LDAP アクセスを設定する手順は以下の通りです。

1. 認証局証明書（CA）をインストールします
2. ドメインコントローラ用の RSA 証明書を生成します。
3. RSA 証明書をサーバにインストールします。

4.4.5.2 iRMC S2 ユーザーのロール　（許可グループ）への割り当て

以下のいずれかにに基づいて、iRMC S2 ユーザーを iRMC S2 許可グループに割り当てます。

– ユーザーエントリ、または、

– ユーザーエントリ／グループエントリ

> **i** 以下の例では、LDAP v2 ストラクチャを使用して、OU「SVS」のロールエントリに基づく割り当てを記述しています。LDAP v1 ストラクチャの場合は、グループエントリは OU「iRMCgroups」に保存されます。
>
> ユーザーエントリに基づく割り当て方法もほぼ同じです。

> **i** Active Directory のグループに「マニュアル」でユーザーを入力する必要があります。

以下の通り進めます :

➤ スナップイン「Active Directory ユーザーとコンピュータ」を開きます。

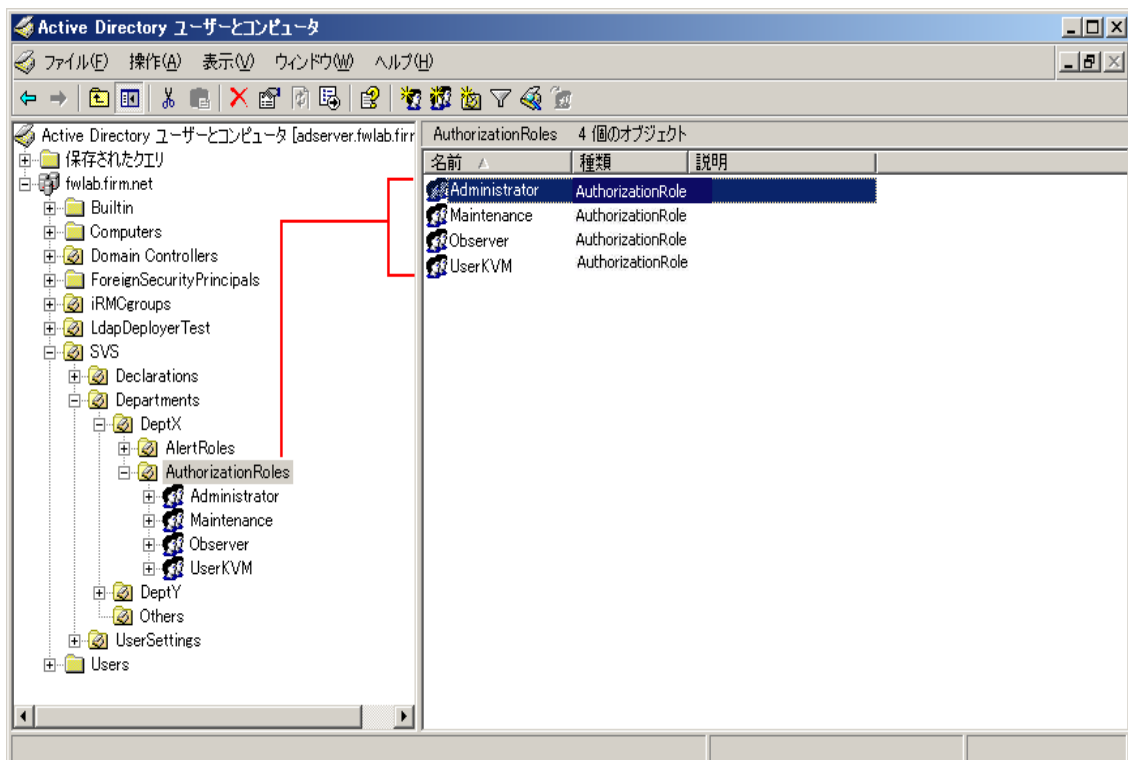



図 32： Active Directory ユーザーとコンピュータスナップイン

➤ 許可グループをダブルクリックします。（この例では Administrator）。

「Administrator のプロパティ」ダイアログが開きます。（図 33 を参照してください。）

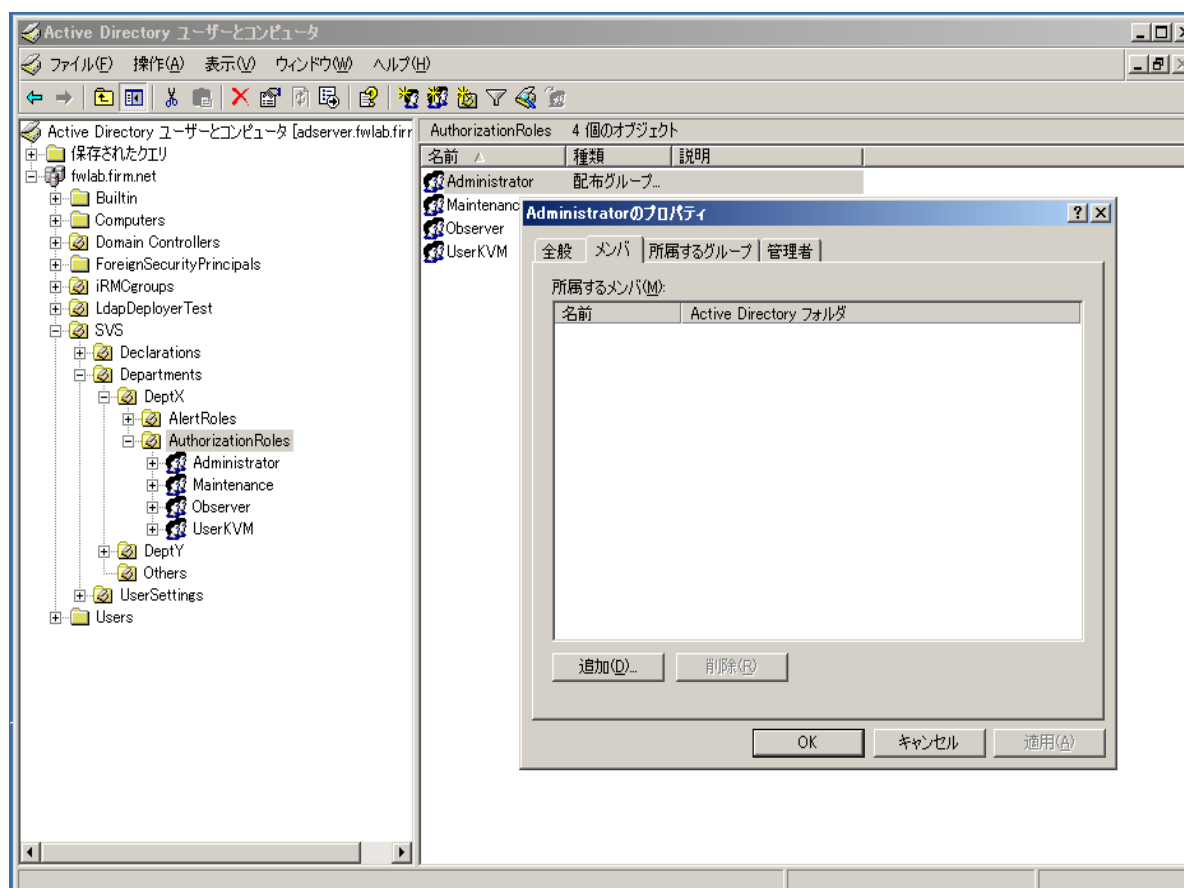



図 33： 「Administrator のプロパティ」ダイアログ

➢ 「メンバ」タブを選択します。

➢ ［追加 ］ボタンをクリックしてください。

「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログが開きます。(図 34 を参照してください。)

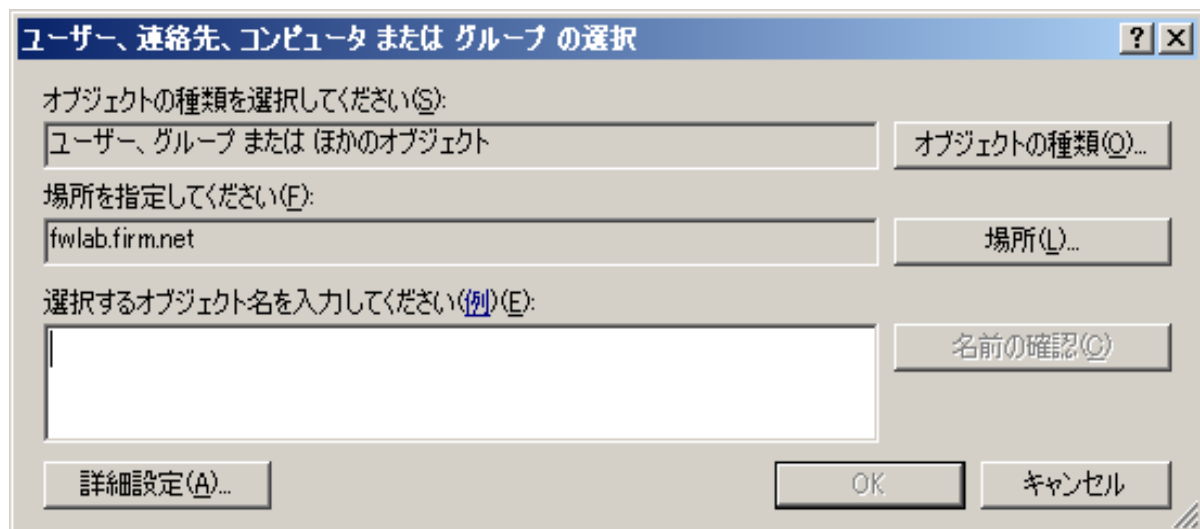



図 34：「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログ

➤ ［場所］ボタンをクリックしてください。

「場所」ダイアログが開きます。

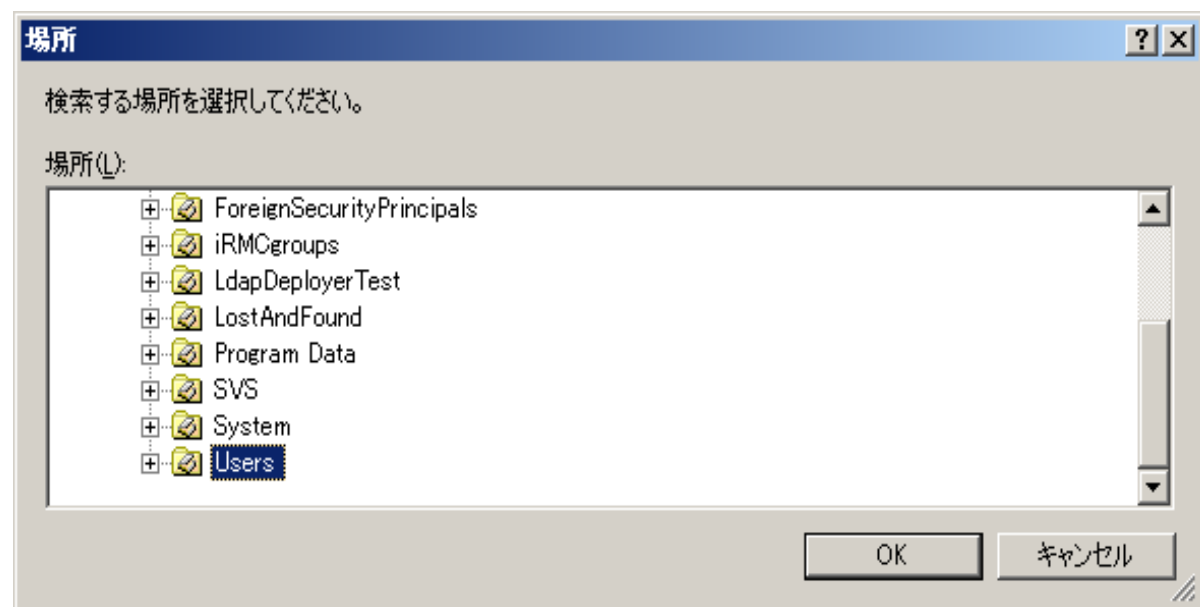



図 35：「場所」ダイアログ

➤ 該当するユーザーを含むコンテナ（OU）を選択してください。（デフォルト値では OU 「Users.」となります。）［OK］をクリックして確定します。

「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログが開きます。(図 36 を参照してください。)

i ディレクトリ内の他の位置にユーザーを入力することもできます。

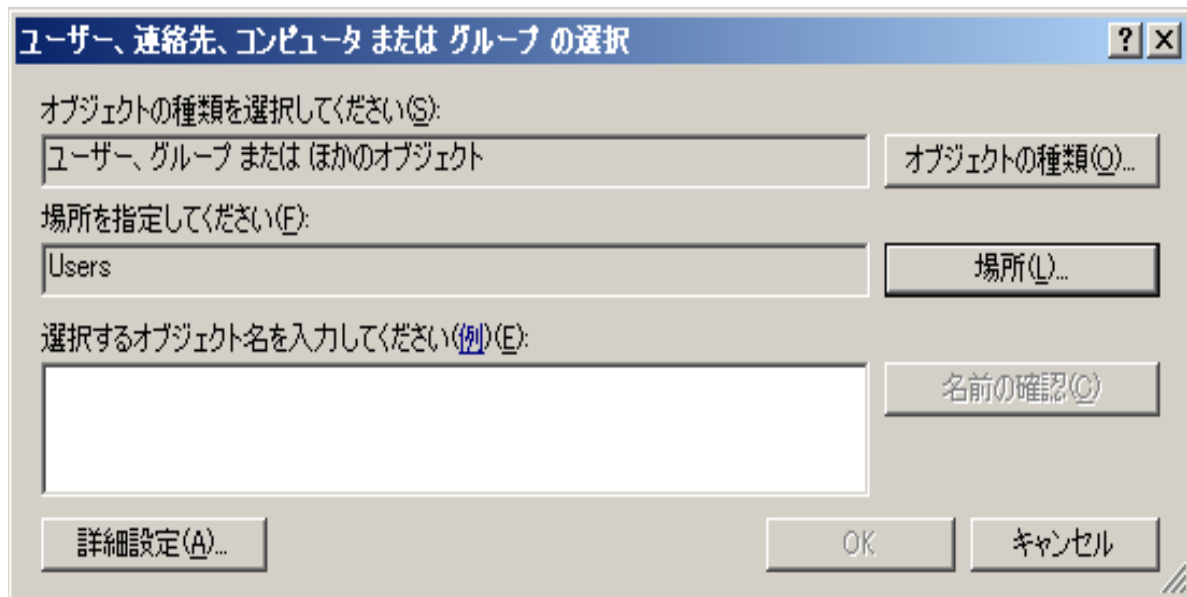



図 36： 「ユーザー、連絡先、コンピュータ または グループの選択」ダイアログ

➤ ［詳細設定 .....］ボタンをクリックしてください。

「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログが展開されます。

（図 37 を参照してください。

図 37 :「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログ - 検索画面

➤ ［今すぐ検索］ボタンをクリックしてドメイン内のすべてのユーザーを表示させます。

「検索結果」の表示部に検索結果が表示されます。（図 38 を参照してください。）

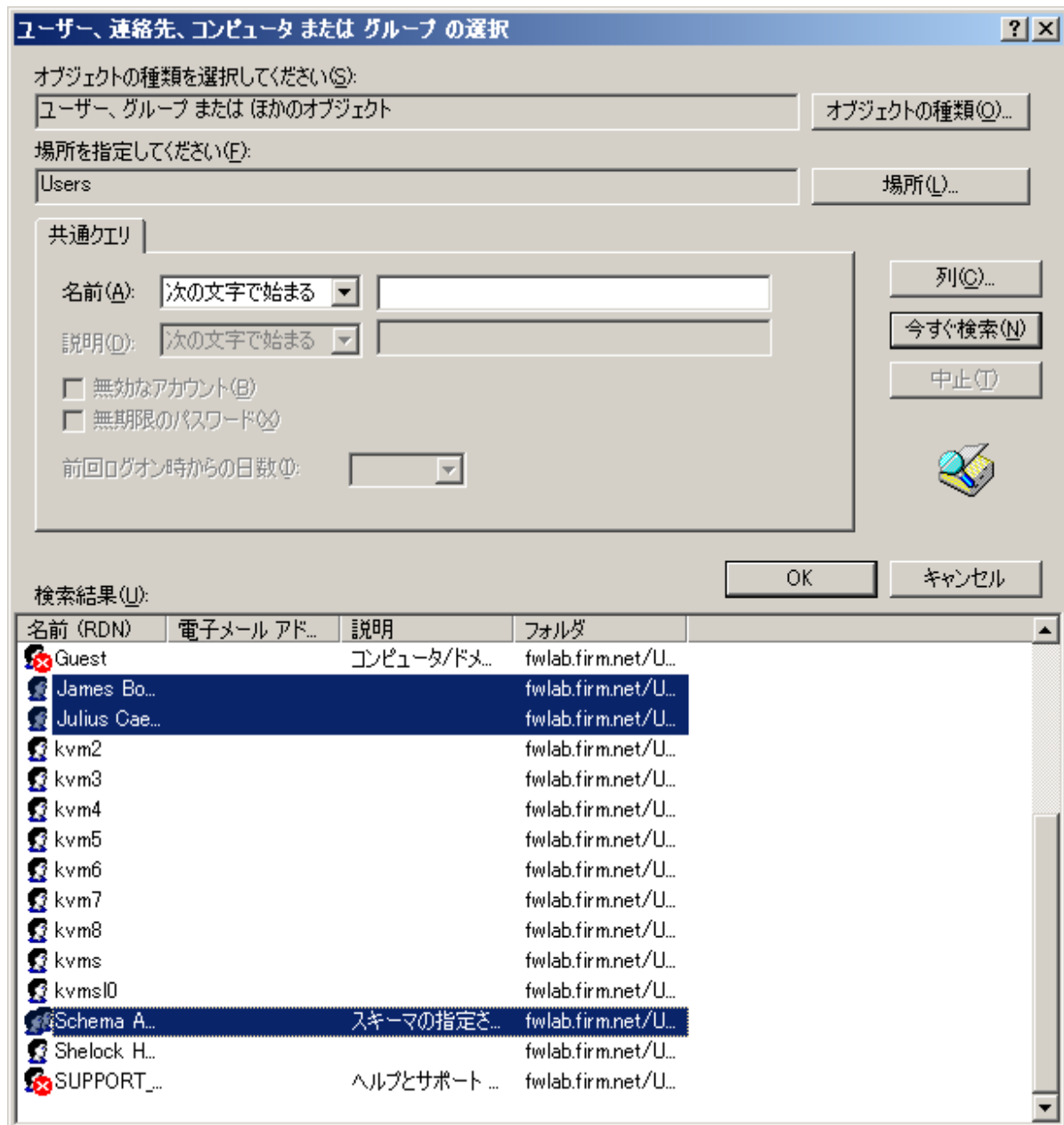



図 38 :「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログ - 検索結果表示

➢ グループに追加するユーザーを選択し、［OK］をクリックして確定します。

選択されたユーザーが表示されます。(図 39 を参照してください。)

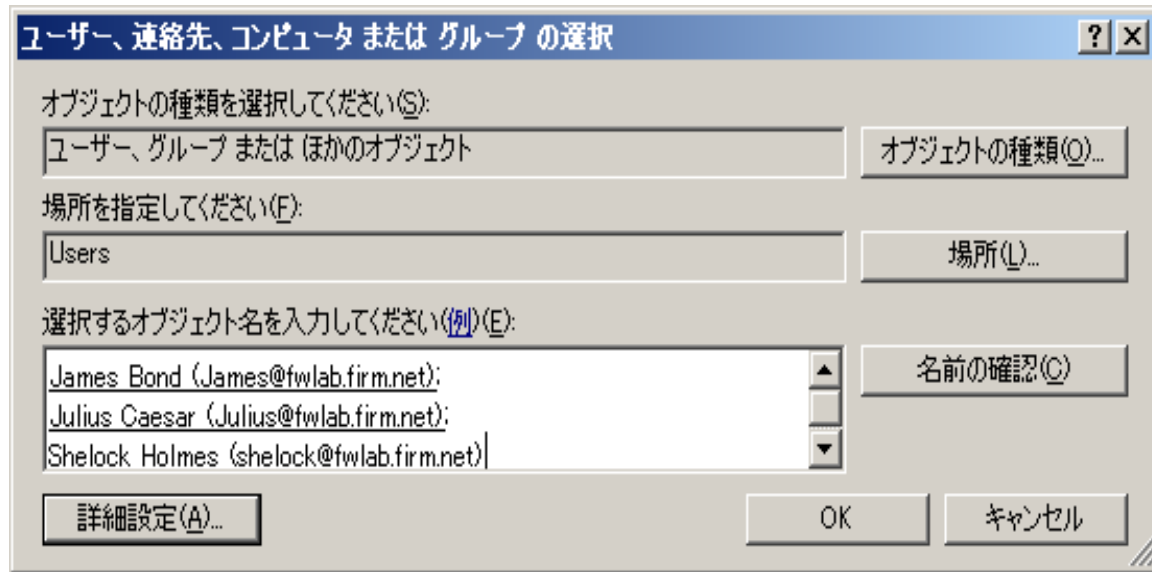



図 39 :「ユーザー、連絡先、コンピュータまたはグループの選択」ダイアログ - 検索結果確認

➤［*OK*］をクリックして確定します。

4.4.6 Novell eDirectory によるグローバル iRMC S2 ユーザー管理

Novell eDirectory は未サポートです。

この節では次の点について説明します。

– Novell eDirectory のシステムコンポーネントとシステム要件

– Novell® eDirectory のインストール（未サポート）

– Novell® eDirectory の設定（未サポート）

– iRMC S2 ユーザー管理の Novell eDirectory への統合（未サポート）

– Novell eDirectory 管理のためのヒント（未サポート）

以下に Novell eDirectory のインストールと設定を詳しく説明します。eDirectory の広範な知識は必要ありません。すでに Novell eDirectory に習熟しているユーザーは以降の 3 つの節を飛ばして、123 ページ「iRMC S2 ユーザー管理の Novell eDirectory への 統合」に進んでください。

4.4.6.1 ソフトウェアコンポーネントとシステム要件

以下にリストされた指定されたバージョン以降のコンポーネントを使用してくださ い。

Novell eDirectory（以前の NDS）は以下のソフトウェアコンポーネントで設定されています。

– eDirectory 8.8: 20060526_0800_Linux_88-SP1_FINAL.tar.gz

– eDirectory 8.8: eDir_88_iMan26_Plugins.npm

– iManager: iMan_26_linux_64.tgz for SuSE, iMan_26_linux_32.tgz otherwise – ConsoleOne: c1_136f-linux.tar.gz

Novell eDirectory をインストールし運用するには以下のシステム要件を満たす必要があります。

– OpenSSL をインストールする必要があります。

OpenSSL がインストール済みでない場合は、

➢ Novell eDirectory をインストールする前に OpenSSL をインストールしてください。

– 512 MB の RAM 空き領域

4.4.6.2 Novell® eDirectory のインストール（未サポート）

Novell eDirectory のインストールには以下のコンポーネントをインストールしてください：

– eDirectory Server と管理ユーティリティ

– iManager （管理ユーティリティ）

– ConsoleOne （管理ユーティリティ）

Novell eDirectory インストールの前提条件 **:**

– Linux サーバ OS のフルインストールと稼働。

– ファイヤーウォールを以下のポートに接続可能な設定にします。

8080, 8443, 9009, 81, 389, 636.

OpenSuSE では「/etc/sysconfig/SuSE firewall2」の中でこの設定を行います。

➢ ファイル「/etc/sysconfig/SuSE firewall2」にエントリ「FW_SERVICES_EXT_TCP」を次のように追加します。

FW_SERVICES_EXT_TCP="8080 8443 9009 81 389 636"

– eDirectory インストールガイドに従ってシステムにマルチキャストルーティングの設定を行います。

SuSE Linux の場合は以下のように進めてください。

➢ ファイル「/etc/sysconfig/network/ifroute-eth0」を作成するか、（作成済みの場合は）開いてください。

➢ 「/etc/sysconfig/network/ifroute-eth0」に以下の行を追加します。

224.0.0.0 0.0.0.0 240.0.0.0 eth0

この操作で eth0 がシステムコンフィグレーションに取り込まれます。

eDirectory Server、**eDirectory** ユーティリティ、**iManager** および **ConsoleOne** インストールの前提条件：

– インストールを実行するにはルート権限が必要です。

– 以下の手順でインストールを実行する前に必要なすべてのファイルをディレクトリ（たとえば「/home/eDirectory」）コピーしておく必要があります。必要なファイルは以下のとおりです。

20060526_0800_Linux_88-SP1_FINAL.tar.gz

iMan_26_linux_64.tgz

c1_136f-linux.tar.gz

Directory Server と管理ユーティリティのインストール

以下の通り進めます :

➢ ルート権限（スーパーユーザー）でログインします。

➢ インストールに必要なファイルが入っているディレクトリに移動します。（この例では「/home/eDirectory」:

cd /home/eDirectory

➢ 「20060526_0800_Linux_88-SP1_FINAL.tar.gz」アーカイブを解凍します。

tar -xzvf 20060526_0800_Linux_88-SP1_FINAL.tar.gz

解凍すると、「/home/eDirectory」に「eDirectory」という名前のサブディレクトリが作られます。

「*eDirectory Server*」のインストール

➢ このディレクトリ「eDirectory」のサブディレクトリ、「setup」に移動します。

cd eDirectory/setup

➢ インストール用スクリプト、「./nds-install」を呼び出してください。

./nds-install

➢「Y」をキーインして EULA を承認し [Enter］キーで確定します。

➢ どのプログラムをインストールするか尋ねられたら

「**install the Novell eDirectory server**」に「1」を入力し、［Enter］キーを押して確定します。

これで、eDirectory パッケージがインストールされます。

Novell eDirectory Server がインストールできたら、eDirectory までのパス名を環境変数で更新し、これらの変数をエクスポートします。

➢ この操作を行うには、設定ファイル（この例では「 /etc/bash.bashrc」）を開き、次の行に指定されたシーケンスを「# End of ...」の前に入力します :

export PATH/opt/novell/eDirectory/bin:/opt/novell/eDirectory/sbin:$PATH

export LD_LIBRARY_PATH=/opt/novell/eDirectory/lib: /opt/novell/eDirectory/lib/nds-modules:/opt/novell/lib:$LD_LIBRARY_PATH

export MANPATH=/opt/novell/man:/opt/novell/eDirectory/man:$MANPATH

export TEXTDOMAINDIR=/opt/novell/eDirectory/share/locale: $TEXTDOMAINDIR

➢ ターミナルを閉じ、新しいターミナルを立ち上げて環境変数をエクスポートします。

eDirectory 管理ユーティリティのインストール

➢ ディレクトリ「eDirectory」のサブディレクトリ、「setup」に移動します。

cd eDirectory/setup

➢ インストール用スクリプトを呼び出します。

./nds-install

➢ 「Y」をキーインして EULA を承認し [Enter] キーで確定します。

➢ どのプログラムをインストールするか尋ねてきたら :

「**install the Novell eDirectory administration utilities**」に「2」を入力し、[Enter] キーを押して確定します。

これで、eDirectory 管理ユーティリティがインストールされます。

iManager のインストールと起動

Novell eDirectory のインストールには iManager を使用することを推奨します。SLES10 または OpenSuSE にインストールする場合は、アーカイブ「*_64.tgz」を使用します。

以下の通り進めます :

➢ ルート権限（スーパーユーザー）でログインします。

➢ ディレクトリ「/home/eDirectory」に移動します。

cd /home/eDirectory

➢ アーカイブ「iMan_26_linux_64.tgz」を解凍します。

tar -xzvf iMan_26_linux_64.tgz

解凍すると、「/home/eDirectory」には「iManager」という名前のサブディレクトリが作られます。

➢ 「iManager」の「installs」サブディレクトリに移動します。

cd iManager/installs/linux

➢ インストール用スクリプトを起動します。

./iManagerInstallLinux.bin

➢ インストール時のメッセージを出力する言語を選択します。

➢ クリックを繰り返し、EULA を承認します。

➢「Novell iManager 2.6, Tomcat, JVM 」を選択して iManager をインストールしてください。

➢ 「Yes」を選択してプラグインをダウンロードします。

➢ ダウンロードにデフォルトのパスを使うには［Enter］キーを押してください。インストールプログラムがインターネット上でダウンロードするサイトを検索します。この処理には数分かかることがあります。次に、どのプラグインをインストールしたいかを尋ねられます。

  ➢ すべてのプラグインをダウンロードするには「All」を選択します。

  ➢ 「1- Yes」を選択して自環境で使用可能なプラグインをインストールします。

➢ インストールに初期値のパスを使う場合は［Enter］キーを押してください。

➢ Apache を自動設定（オプション）させるには「2- No」を選択します。

➢ Tomcat にはデフォルトポート（8080）を承認します。

➢ Tomcat にデフォルト SSL ポート（8443）を承認します。

➢Tomcat にデフォルト JK コネクタポート（9009）を承認します。

➢ 適切な管理権限を持つ管理ユーザーの ID（たとえば「root.fts」）を入力してください。

➢ 適切な管理権限を持つ管理ユーザーのツリー名（たとえば「rfwlab」）を入力してください。

➢「1-OK..」と一緒に表示されたエントリの要約を承認してインストールを終了させます。

「*Novell iManager*」へのログイン

インストールが終われば、以下の URL からウェブブラウザ経由で iManager にログインできます。

https://<IP address of the eDirectory server>:8443/nps

Novell のブラウザには Microsoft Internet Explorer または Mozilla Firefox を推奨します。Mozilla Firefox であれば、一度にすべてのコンテキストメニューのポップアップウィンドウを表示させないようにすることもできます。

ConsoleOne のインストールと起動

ConsoleOne は Novell eDirectory のもうひとつの管理ツールです :

ConsoleOne を以下のようにインストールしてください。

- ➢ ディレクトリサーバにルート権限（スーパーユーザー）でログインします。
- ➢ ディレクトリ「/home/eDirectory」に移動します。

  cd /home/eDirectory
- ➢ ConsoleOne のアーカイブ「c1_136f-linux.tar.gz」を解凍します。

  tar -xzvf c1_136f-linux.tar.gz

  解凍すると、「/home/eDirectory」に「Linux」という名前のサブディレクトリが作られます。
- ➢ ディレクトリ「Linux」に移動します。

  cd Linux
- ➢ インストール用スクリプト、「c1-install:」を呼び出してください。

  ./nds-install
- ➢ インストールのメッセージを出力する言語を選択します。
- ➢ 「8」を入力してすべてのスナップインをインストールしてください。

ConsoleOne にはインストール済みの Java ランタイム環境へのパスが必要です。対応するパス名を環境変数「C1_JRE_HOME」にエクスポートすることができます。ただし、パス名をシステム全体にエクスポートするためには「bash」プロファイルの変更が必要です。

i ConsoleOne を操作するためには原則として ID「superuser Root」をエクスポートできるレベルのルート権限が要求されます。パス名をシステム全体にエクスポートする方法は以下に紹介する通りです。すなわち、通常のユーザーでもルート権限があれば ConsoleOne を操作することができます。

以下の通り進めます :

- 編集する設定ファイルを開きます。(この例では 「/etc/bash.bashrc」)
- 設定ファイルの「# End of ...」の前に次の行を入力します。

export C1_JRE_HOME=/opt/novell/j2sdk1.4.2_05/jre

eDirectory と同時にインストールされた Java ランタイム環境をここで使用します。一方、eDirectory Server 上にインストールされたいずれかの Java ランタイム環境のパス名を指定することもできます。

ConsoleOne はローカルの設定ファイル「hosts.nds」または SLP サービスとマルチキャストを経由して使用可能なツリー階層を取得します。

以下のように、ユーザーのツリー階層を設定ファイルに挿入してください。

- 設定用ディレクトリに移動します。

  cd /etc

- ファイル「hosts.nds」がまだ存在しない場合には作成してください。
- ファイル「hosts.nds」を開いて以下の行を挿入します。

  #Syntax: TREENAME.FQDN:PORT

  MY_Tree.mycomputer.mydomain:81

ConsoleOne の起動

ConsoleOne はシステムプロンプトから以下のコマンドを使用して起動できます。

/usr/ConsoleOne/bin/ConsoleOne

4.4.6.3 Novell® eDirectory の設定（未サポート）

以下の手順を実行して Novell eDirectory を設定してください。

1. NDS ツリーの作成
2. eDirectory の LDAP 用設定
3. LDAP ブラウザを経由した eDirectory の試験アクセス

NDS ツリーの作成

ndsmanage ユーティリティを使用して NDS（**N**etwork **D**irectory **S**ervice）を作成します。この作業を行うために、ndtmanage には以下の情報が必要です。

ツリー名

新しい NDS ツリー用のネットワーク用の一意の名前、たとえば「MY_TREE」

サーバ名

eDirectory 内の「server」クラスのインスタンス名。「Server Name」には、LDAP サーバが稼働している PRIMERGY サーバの名前、たとえば、「lin36-root-0」を指定してください。

サーバコンテキスト

「server」オブジェクトを格納するコンテナの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、
dc=organization.dc=mycompany.

Admin ユーザー

管理を実行する許可を持つユーザーの完全な識別名（オブジェクトパスと属性の完全な識別名）、たとえば、

cn=admin.dc=organization.dc=mycompany

NCP ポート

ポート 81 を指定してください。

インスタンスのロケーション

パスを指定してください。*/home/root/instance0*

設定ファイル

以下のファイルを指定してください。*/home/root /instance0/ndsconf*

Admin ユーザーのパスワード

管理者のパスワードをここに入力します。

次の手順で NDS ツリーを設定します。

➢ コマンドボックスを開きます。

➢ ディレクトリ「/home/eDirectory」に移動します。

➢ 「ndsmanage」コマンドを入力して「ndsmanage」ユーティリティを起動します。

ndsmanage

➢ 「C」を入力してクラス「server」の新しいインスタンスを生成します。

➢ 「Y」を入力して設定作業を続けます。

➢ 「Y」を入力して新しいツリーを作成します。

次に、「ndsmanage」から、順番に「TREE NAME」、「Server Name」、「Server Context」などの値が尋ねられます。(117 ページを参照してください。)

入力が完了すると NDS ツリーが 「ndsmanage」によって設定されます。

➢ NDS ツリーの設定が終わったら、PRIMERGY サーバを再起動させて、設定の実効化、すなわち、NDS ツリーの再作成を行います。

eDirectory for LDAP の設定

eDirectory for LDAP を設定する手順は以下の通りです。

– Role Based Services （RBS）のインストール

– プラグインモジュールのインストール

– Role Based Services （RBS）の設定

– eDirectory の設定（SSL/TLS を使用する、もしくは、使用しない）

以下の手順で個々の作業を完了させます。

➢ ブラウザを使用して、管理者 ID（Admin）で iManager にログインします。

Role Based Services （*RBS*）のインストール

iManager Configuration ウィザードを使って RBS をインストールします。

以下の通り進めます。

- iManager で、「Configure」タブを選択します（「desk」アイコンをクリックしてください）。
- 「Configure」タブから以下を選択します Role Based Services - RBS Configuration
- 「RBS Configuration」ウィザードを起動してください。
- 作業を行うコンテナに「RBS2」を 割り当ててください。（上記の例では「mycompany」となっています。）

プラグインモジュールのインストール

以下の通り進めます :

- iManager で、「Configure」タブを選択します（「desk」アイコンをクリックしてください）。
- 「Configure」タブで次の通り選択します

  Plug-in installation - Available Novell Plug-in Modules
- 「Available Novell Plug-in Modules」ページにリストされたモジュールから、eDirectory 専用のパッケージ「eDir_88_iMan26_Plugins.npm」を選択します。
- ［Install］をクリックします。

  Role Based Services（*RBS*）の設定
- 「Available Novell Plug-in Modules」ページで、LDAP 統合に必要なモジュールをすべて選択してください。よくわからない場合は、すべてのモジュールを選択します。
- ［Install］をクリックします。

eDirectory の *SSL/TLS-* セキュリティ保護されたアクセスの設定

> i eDirectory のインストール中には、臨時の証明書が生成されますので、eDirectory へのアクセスは初期設定でも SSL/TLS セキュリティ保護されます。
>
> ただし、iRMC S2 のファームウェアは RSA/MD5 証明書を使用するように設定されているので、SSL/TLS セキュリティ保護された eDirectory 経由のグローバル iRMC S2 ユーザー管理には 1024 バイト長の RSA/MD5 証明書が必要です。

1024 バイト長の RSA/MD5 証明書は ConsoleOne を使用して以下のように作成します :

- 管理者 ID（Admin）を使用して、LDAP サーバにログインし、ConsoleOne を起動してください。
- コーポレートストラクチャのルートディレクトリに移動してください。
  （たとえば、「*treename/mycompany/myorganisation*」）
- 「*New Object - NDSPKI key material - custom*」を選択して、クラス「NDSPKI:Key Material」の 新しいオブジェクトを作成します。
- その後に表示されるダイアログで、以下の数値を指定してください。
  1. 1024 bits
  2. SSL または TLS
  3. RSA/MD5 のサイン

要求されるタイプのサインを新しく作る必要があります。

SSL セキュリティ保護された LDAP 接続のために新たに作成した証明書を有効化するには、iManager で以下の作業を実行します。

- ウェブブラウザから iManager を起動します。
- 有効な認証データを使用して iManager にログインします。
- 「*LDAP*」→「 *LDAP Options*」→「 *LDAP Server*」→「 *Connection*」の順で選択します。

  「Connection」タブにはシステム上でインストールされたすべての証明書を表示するドロップダウンリストがあります。
- ドロップダウンリストから必要な証明書を選択します。

eDirectory の *SSL/TLS-* セキュリティ保護されないアクセスの設定

eDirectory のデフォルト設定では匿名ログインやセキュリティ保護されないチャンネルを経由する平文表示のパスワードは無効となります。このため、eDirectory サーバ にウェブブラウザでログインするには SSL コネクション経由とするほかには方法があ りません。

LDAP を SSL なしで使用したい場合は、以下の手順を実行しなければなりません。

1. SSL セキュリティ保護されない LDAP 接続の確立
2. バインド制限の緩和
3. LDAP 設定の再ロード

以下の通り進めます。

1. SSL セキュリティ保護されない LDAP 接続の確立

   ➢ ウェブブラウザから iManager を起動します。

   ➢ 有効な認証データを使用して iManager にログインします。

   ➢「*Roles and Tasks*」ビューを選択します。

   ➢「*LDAP*」→「 *LDAP Options*」→「 *LDAP Server*」→「 *Connection*」の順で選択します。

   ➢「Connection」タブで、「*Require TLS for all Operations.*」オプションを無効にします。

   ➢「*LDAP*」→「 *LDAP Options*」→「*LDAP Group* 」→「 *General*」の順で選択します。

   ➢「*Genera*」l タブで「*Require TLS for Simple Binds with password.*」オプションを無効にします。

2. バインド制限の緩和

   ➢ 有効な認証データを使用して iManager にログインします。

   ➢ オブジェクトツリーの中で「*LDAP Server*」オブジェクトに移行します。

   ➢ マウスで「*LDAP Server*」オブジェクトをクリックしてハイライトさせ、関連するコンテキストメニューから「*Modify Object*」を選択します。

   ➢ 右側のコンテンツフレームから「*Other*」シートを開きます。

   ➢「*Valued Attributes*」の下から「*ldapBindRestrictions*」を選択します。

   ➢［*Edit* ］ボタンをクリックしてください。

   ➢ 数値を「0」に設定します。

   ➢［*OK*］をクリックします。

   ➢「*Other*」シートで［*Apply*］ボタンをクリックします。

3. LDAP 設定の再ロード

   ➢ ConsoleOne を起動して eDirectory にログインしてください。

   ➢ ウィンドウ左側の「*Base DN*」オブジェクト（たとえば、「Mycompany」）をクリックします。すると「*LDAP server*」オブジェクトがウィンドウの右側に表示されます。

   ➢ 右クリックして「*LDAP Server*」オブジェクトをハイライトさせ、関連するコンテキストメニ ューから「*Properties...*」を選択します。

   ➢「General」タブで「*Refresh NLDAP Server Now*」クリックします。

LDAP からブラウザへの **eDirectory** アクセス試験

以上 1 から 3 までの手順に成功したら、LDAP ブラウザユーティリティを使用して、eDirectory への 接続を確立しなければなりません。Jarek Gavor 氏 の LDAP ブラウザ （139 ページ参照）を使用して、以下のようにこの接続の試験をします。

➢ 管理者 ID（ たとえば admin）を使用して SSL 接続経由で eDirectory に接続できるか試してみます。この接続に失敗した場合は、以下のようにしてください。

➢ SSL が有効であることを確認します。（120 ページを参照してください。）

図 40： eDirectory への LDAP 接続の試験： SSL 有効時

➢ 管理者 ID （たとえば admin）を使用してセキュリティ設定のない SSL 接続経由で eDirectory にログインできるか試してみます。

図 41 : eDirectory への LDAP 接続の試験 : SSL 無効時

➤ 再度ログインに失敗したら。

バインド制限を緩和します（120 ページを参照してください）。

4.4.6.4 iRMC S2 ユーザー管理の Novell eDirectory への統合（未サポート）

前提条件 :

LDAP v1 もしくは、LDAP v2 ストラクチャ が eDirectory ディレクトリサービスの中に生成済みであること。（90 ページの「SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除」の節を参照してください。）

以下の手順を実行して、iRMC S2 ユーザー管理を Novell eDirectory に統合します。

– iRMC プリンシパルユーザーの作成

– eDirectory の iRMC グループとユーザー許可の宣言

– ユーザーを許可グループ割り当て

eDirectory の iRMC S2 ユーザー LDAP 認証プロセス

グローバル iRMC S2 ユーザーが iRMC S2 にログインする際の認証は、定義済みのプロセスに従って処理されます（54 ページを参照してください）。図 42 は Novell eDirector のグローバル iRMC S2 ユーザーを管理するプロセスを図解したものです。

対応するログイン情報による接続とログインの確立を、BIND 操作と呼びます。

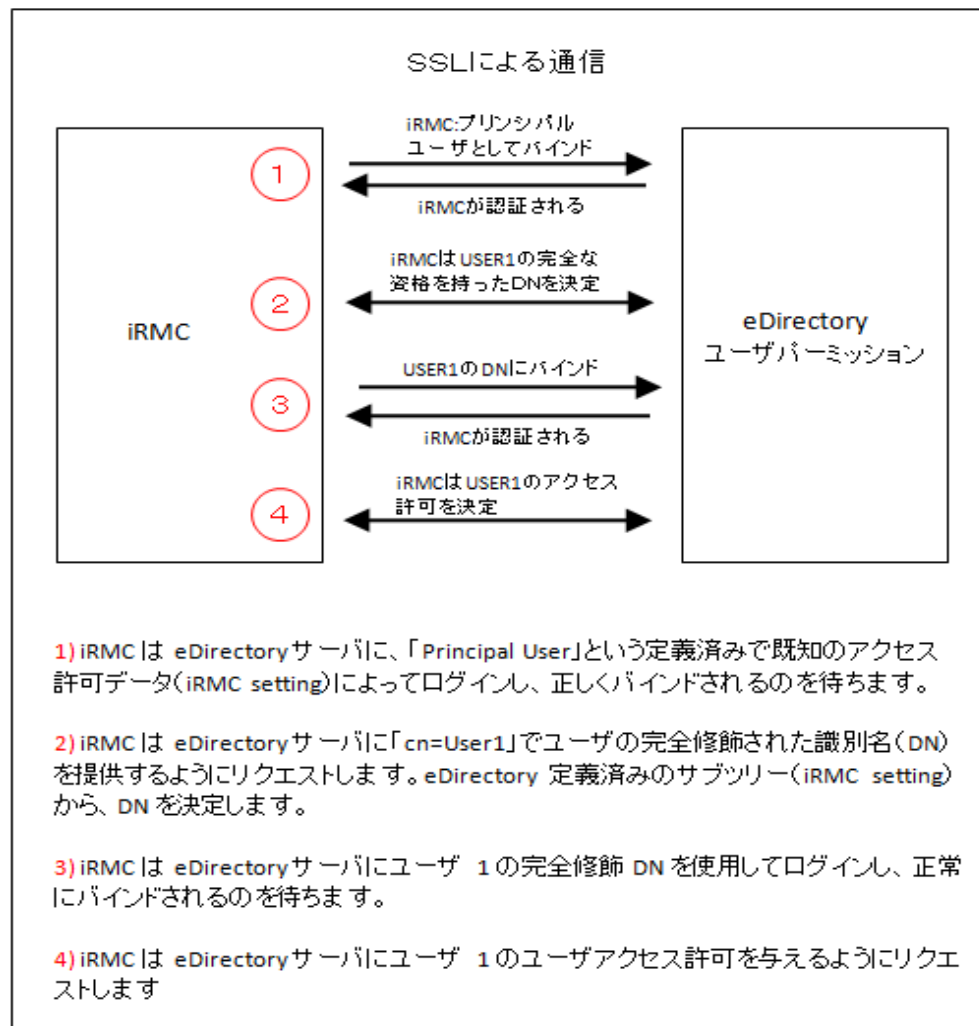



図 42： グローバル iRMC S2 の許可の認証ダイアグラム

「プリンシパルユーザー」の許可データとサブツリーが設定され、その中には、iRMC S2 の Web インターフェースのページである「Directory Service Configuration」ページの中の DN が含まれます。(321 ページを参照してください。)

ユーザーの CN は検索されるサブツリーの中で一意でなければなりません。

iRMC S2 用のプリンシプルユーザーの作成

iRMC S2 用のプリンシプルユーザーを以下の通り作成します。

- ➢ 有効な認証データを使用して iManager にログインします。
- ➢「Roles and Tasks」を選択します。
- ➢「Users - Create User」を選択します。
- ➢ 表示されるテンプレートに必要な項目を入力します。

プリンシパルユーザーの識別名（DN）とパスワードは、対応する iRMC S2 の設定の項目に一致しなければなりません。(321 ページ、「ディレクトリサービス設定（LDAP）– iRMC S2 のディレクトリサービスの設定」の節を参照してください。)

ユーザーの「Context:」はツリーのどの位置にあっても構いません。

- ➢ 以下のサブツリーにプリンシパルユーザーの検索許可を割り当てます。
  - – サブツリー (OU)「iRMCgroups」または「SVS」
  - – ユーザーを含むサブツリー (OU)（たとえば「people」）

iRMC グループとユーザーへのユーザー許可の割り当て

デフォルト設定では、eDirectory のオブジェクトには、LDAP ツリー内の非常に限定されたクエリと検索の許可しかありません。ひとつまたは複数のサブツリーのすべての属性をオブジェクトがクエリできるようにするには、このオブジェクトに対応する許可を割り当てる必要があります。

許可は個々のオブジェクト（すなわち個々のユーザー）に割り当てることもできますし、「*iRMCgroups / SVS*」または「*people*」のような同じ組織単位（OU）に照合されるオブジェクトのグループに割り当てることもできます。この場合は、OU に割り当てられ、「引き継がれた」と識別された許可は、このグループのオブジェクトに自動的に認定されます。

iRMC S2 のユーザー管理と Novell eDirectory を統合するには、次のオブジェクト（トラスティ）に検索の許可を割り当てる必要があります。

– プリンシパルユーザー

– iRMC S2 ユーザーが含まれるサブツリー

以下にこの操作を詳しく説明します。

すべての属性にオブジェクト検索許可を割り当てるプロセスは以下の通りです：

➤ ウェブブラウザから iManager を起動します。

➤ 有効な認証データを使用して iManager にログインします。

➤ iManager で［*Roles and Tasks*］ボタンをクリックします。

➤ メニューのツリーストラクチャから「*Rights*」→「 *Rights to Other Objects*」の順で選択します。

「Rights to Other Objects」のページが表示されます。

➤「Trustee Name」の下に、アクセス許可を許可するオブジェクトの名前を指定します。（図 43 の「*iRMCgroups.sbrd4*」および「*SVS.sbdr4*」。）

➤「Context to Search From」の下に「*eDirectory*」のサブツリー（「*iRMCgroups /SVS*」）を指定します。iManager はこのサブツリーから、トラスティ「*Users*」が現在読み取りの許可を持っているオブジェクトすべてを検索します。

➤［*OK*］をクリックしてください。

進捗ディスプレイが検索の状況を表示します。検索作業か終了すると、「*Rights to Other Objects*」のページが、検索結果と合わせて表示されます。（図 43 を参照してください。）

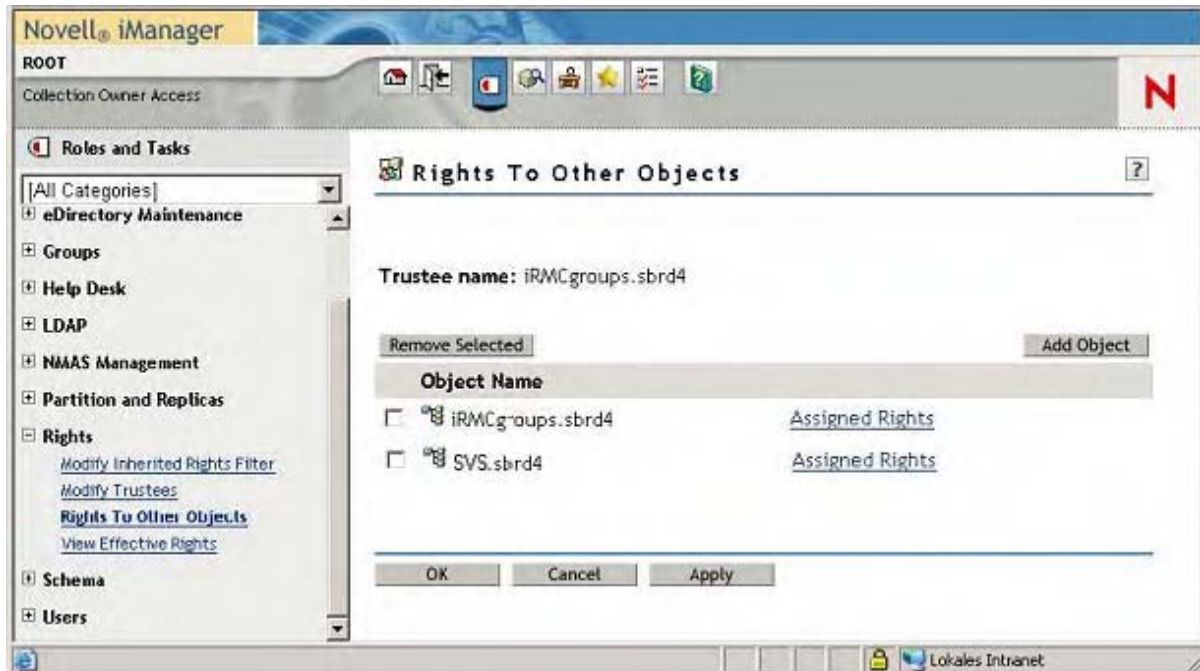



図 43 : iManager - ロールとタスク - 他のオブジェクトに対する権限

「*Object Name*」の下になにもオブジェクトが表示されない場合は、トラスティには現在指定されたコンテキストの範囲内に許可はありません。

- 必要に応じてトラスティに追加の許可を割り当ててください。
  - 「*Add Object*」をクリックします。
  - ［*object selector*］ボタン を使用して、トラスティに許可を割り当てたいオブジェトを選択します。
  - 「*Assigned Rights*」をクリックします。「*All Attributes Rights*」プロパティが表示されない場合は。
    - [Add Property] をクリックします。 「*Add Property*」ウィンドウが表示されます（図 44 を参照してください。）

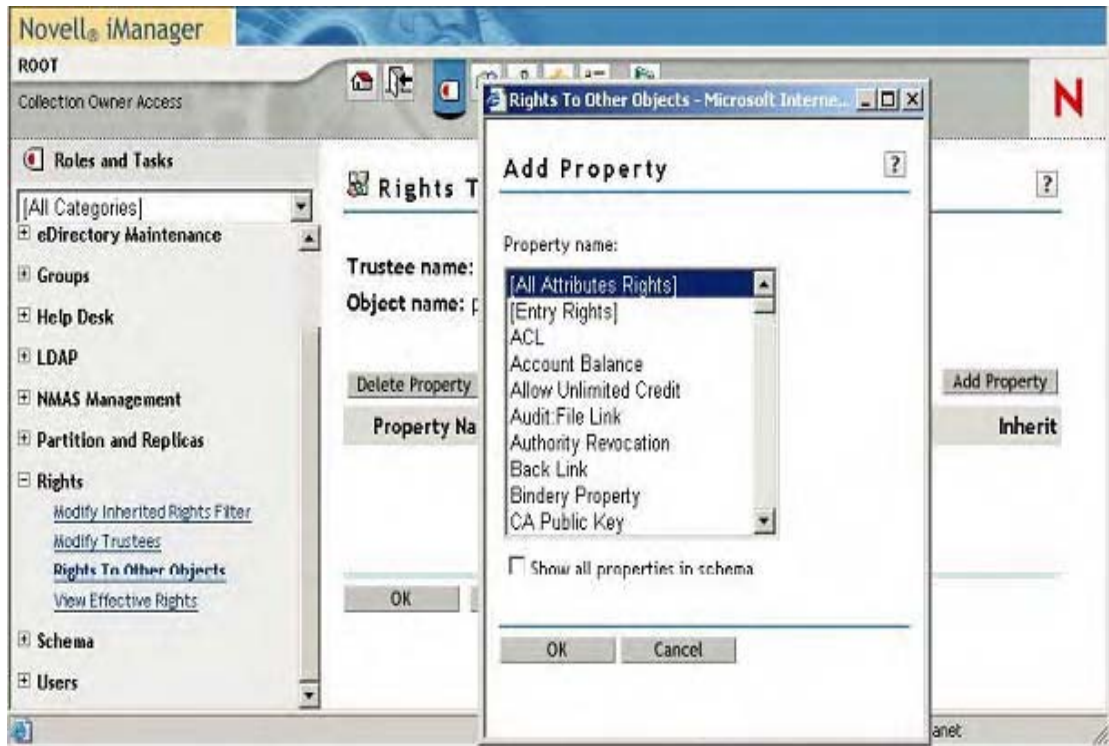



図 44： iManager - ロールとタスク - 他のオブジェクトに対する権限 - プロパティの追加

➢「*All Attributes Rights*」プロパティをハイライトさせ、［OK］クリックして追加します。

➢「*All Attributes Rights*」プロパティの「*Compare*」、「*Read*」および「*Inherit*」オプションを有効にし、［*OK*］をクリックして確定します。

この操作によって、ユーザーまたはユーザーグループに選択されたオブジェクトのサブツリー の属性をすべてクエリする権限を与えられます。

➢［*Apply*］をクリックして設定を有効にしてください。

4.4.6.5 iRMC S2 ユーザーへの許可の割り当て（未サポート）

iRMC S2 ユーザーを（たとえば、OU 「people」から）以下のいずれかの方法で、iRMC 許可グループに割り当てる事ができます。

– ユーザーエントリから開始する（ユーザーエントリが少ない場合に適した方法)、または、

– ロールエントリ／グループエントリから開始する（ユーザーエントリが多い場合に適した方法）

次の例は OU「people」 から許可グループに、iRMC S2 ユーザーを割り当てる方法を示します。割り当てをロールエントリ／グループエントリから開始する方法を説明します。

ユーザーエントリに基づく割り当て方法もほぼ同じです。

eDirectory のグループに「マニュアル」でユーザーを入力する必要があります。

以下の通り進めます :

➢ ウェブブラウザから iManager を起動します。

➢ 有効な認証データを使用して iManager にログインします。

➢「*Roles and Tasks*」を選択してください。

➢「*Groups - Modify Group*」を選択します。*Modify Group* ページが表示されます。

➢ iRMC S2 ユーザーを割り当てたいすべての許可グループについて次の作業を実行します

➢［*object selector*］ボタンを 使用して、iRMC S2 ユーザーを追加したい許可グループを選択します。

– LDAP v1 ストラクチャの例（図 45 参照）ではこの操作は、*Administrator.DeptX.Departments.iRMCgroups.sbrd4.*

– LDAP v2 ストラクチャの例（図 46 参照）ではこの操作は、*Administrator.AuthorizationRoles.DeptX.Departments.SVS.sbrd4*.

➢「*Members* 」タブを選択します。

「*Modify Group*」ページの「*Members*」タブが表示されます。

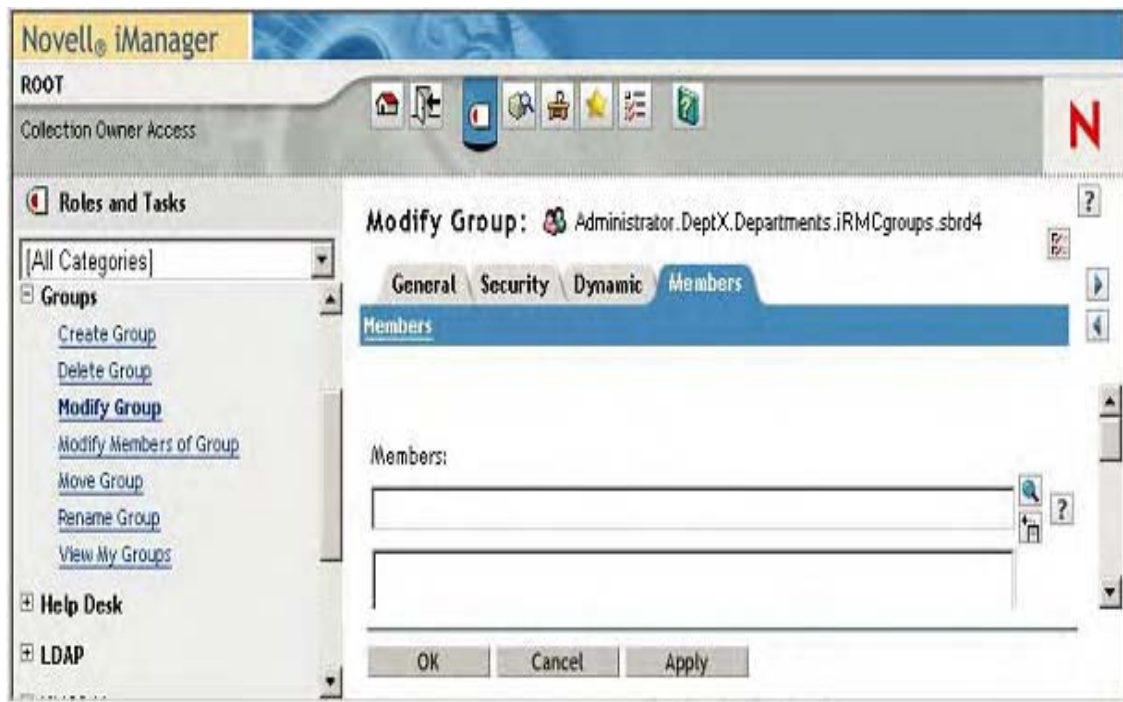



図 45 :「iManager」-「Roles and Tasks」-「Modify Group」-「Members」タブ（LDAP v1）

図 46 :「iManager」-「Roles and Tasks」-「Modify Group」-「Members」タブ（LDAP v2）

➤ iRMC グループに割り当てたいすべての OU 「people」のユーザーについて次の作業を実行します :

➤ ［Object Selector］ ボタンをクリックします。

「Object Selector」（ブラウザ）ウィンドウが開きます（図 47 を参照してください

図 47： iRMC グループへのユーザーの割り当て - ユーザーの選択

➤ 「*Object Selector*」(ブラウザ) ウィンドウで OU「*people*」の中の必要なユーザーを選択し、[*OK*] をクリックして確定します。

選択されたユーザーは「*Modify Group*」ページの「*Members*」タブ表示部にリストされています。(図 48 を参照してください。)

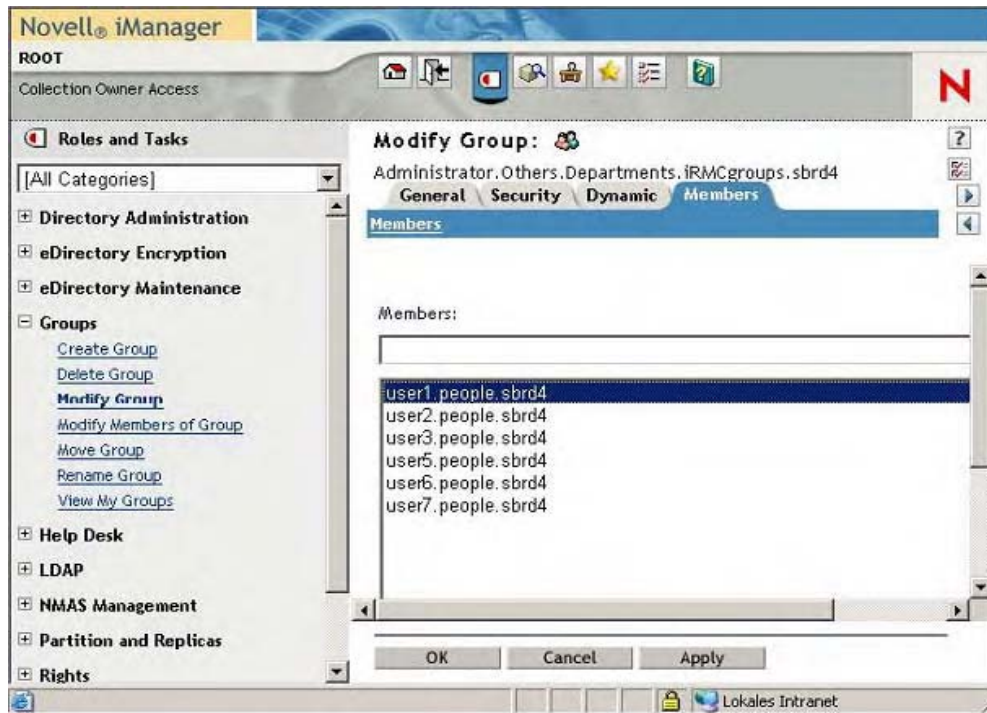



図 48 :「Members LDAP v1」タブが選択された iRMC S2 ユーザー表示

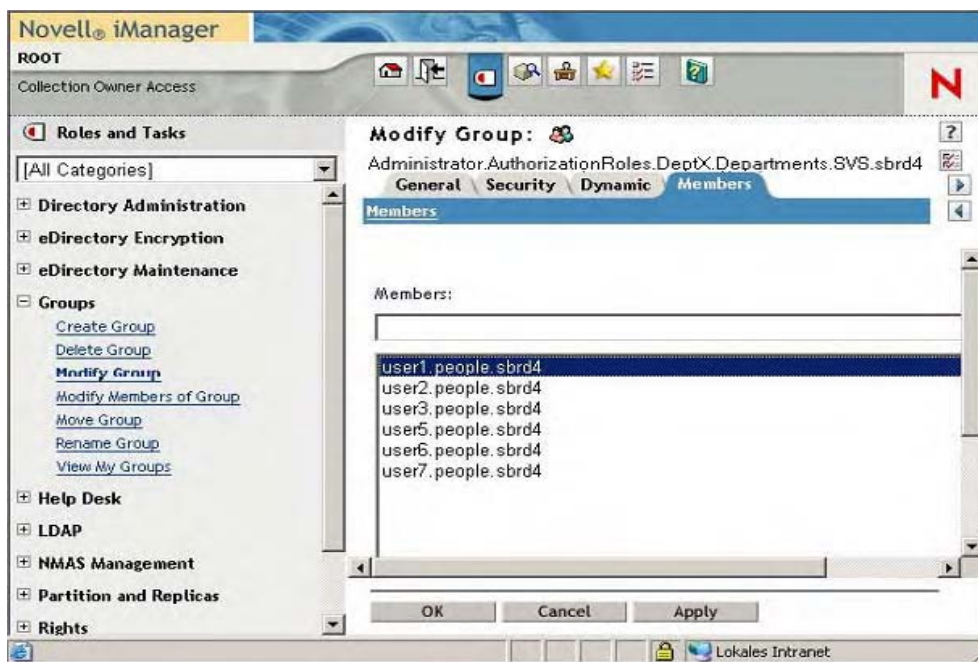



図 49 : 「Members LDAP v2」タブが選択された iRMC S2 ユーザー表示

➢ 選択されたユーザーが iRMC グループに追加されるように、「*Apply*」または［*OK*］で確定してください。（この例では、「*... .iRMCgroups.sbrd4*」または「*... .SVS.sbrd4*」）

4.4.6.6 Novell eDirectory 管理のためのヒント（未サポート）

NDS デーモンの再起動

次の手順で *NDS* デーモンを再起動します *:*

- コマンドボックスを開きます。
- ルート権限でログインします。
- 次のコマンドを実行します。

  `rcndsd restart`

「*nldap*」デーモンの再起動に失敗し、理由が分からない場合は、

- 「Indap」デーモンを「マニュアル」で起動します :

  /etc/init.d/nldap restart

IManager からの応答がない場合は *:*

- iManager を再起動してください。

  /etc/init.d/novell-tomcat4 restart

NLDAP サーバ設定の再ロード

以下の通り進めます :

- ConsoleOne を起動して eDirectory にログインしてください。

ConsoleOne を初めて立ち上げる場合には、ツリーは設定されていません。次の手順でツリーを設定します。

- 「My World」の下のノード NDS を選択してください。
- メニューバーで選択します。「File - Authenticate」
- 次のログイン用認証データを入力します。

1. ログイン名 :「root」
2. パスワード : <password>
3. ツリー :「MY_TREE」
4. コンテキスト :「mycompany」

➢ ウィンドウの左側部分の Base *DN* オブジェクト（「Mycompany」）をクリックします。

すると「*LDAP Server*」オブジェクトがウィンドウの右側に表示されます。

➢「*LDAP Server*」オブジェクト右クリックして、コンテキストメニューの「Properties...」を選択します。

➢「*General*」タブで［*Refresh NLDAP Server Now*］ボタンをクリックします。

NDS メッセージトレース の設定

「*nds*」デーモンがデバッグを行い、ログメッセージを作製します。このメッセージは「*ndstrace*」ツールを使用してトレースすることができます。以下に説明する設定の目的は、「*ndstrace*」の出力をリダイレクトして、他のターミナルでこのファイルを取り込んで表示させることです。後者の作業には 「*screen*」ツールを使用します。

以下の手順を推奨します :

➢ コマンドボックス（たとえば「*bash*」）を開きます。

「*ndstrace*」を設定します

➢「*eDirectory*」の「*/home/eDirectory*」に移動します :

cd /home/eDirectory

➢「*screen*」コマンドを使用して「*screen*」を起動します。

➢「*ndstrace*」コマンドを使用して「*ndstrace*」を起動します。

➢ 有効化したいモジュールを選択します。たとえば、イベントが発生した時間を表示したい場合は、次のように入力します。

dstrace TIME.

LDAP および TIME モジュールを有効化するには、以下のエントリによって行うことを強く推奨いたします。

dstrace LDAP TIME

➢「quit」を入力して「*ndstrace*」を終了させます。
この操作により、「*ndstrace*」の設定作業は終了です。

別のターミナルでメッセージを出力

- 「*ndstrace*」を起動して、メッセージ出力をリダイレクトしてください :

  ndstrace -l >ndstrace.log

- 以下の連結キーを使用して別のターミナルを開きます :

  ［Ctrl］+［a］、［Ctrl］+［c］

- ログの記録を開始させます :

  tail -f ./ndstrace.log

- 仮想ターミナル間の切り替えには、次の連結キーを使用します［Ctrl］+［a］、［Ctrl］+［0］。
  （ターミナルは 0 から 9 まで番号が付けられています。）

4.4.7 OpenLDAP によるグローバル iRMC S2 ユーザーの管理

この節では次の点について説明します :

– OpenLDAP （Linux）のインストール

– SSL 証明書の作成

– OpenLDAP の設定

– iRMC S2 ユーザーの管理の OpenLDAP への統合

– OpenLDAP 管理のヒント

4.4.7.1 OpenLDAP のインストール

i　OpenLDAP をインストールする前に、ファイヤーウォールをポート 389 と 636 に接続できるように設定する必要があります。

4.4.7.2 SSL 証明書の作成

以下のプロパティを持つ証明書を作成する必要があります :

– 鍵の長さ： 1024 ビット

– md5RSAEnc

鍵ペアとサイン入りの証明書（自己サインまたは外部 CA のサイン）の作成には OpenSSL を使用します。より詳しい情報は OpenSSL のホームページ、http://www.openssl.org を参照してください。

CA の設定とテスト証明書の作成の説明書は以下のリンクから入手してください。

– http://www.akadia.com/services/ssh_test_certificate.html

– http://www.freebsdmadeeasy.com/tutorials/web-server/apache-ssl-certs.php

– http://www.flatmtn.com/computer/Linux-SSLCertificates.html

– http://www.tc.umn.edu/~brams006/selfsign.html

証明書の作成に続いて、以下の 3 個の **PEM** ファイルを入手してください。

– ルート証明書： root.cer.pem

– サーバ証明書： server.cer.pem

– 秘密鍵： server.key.pem

> 秘密鍵はパスフレーズで暗号化しないでください。「*server.key.pem*」ファイルには、**LDAP** デーモン（*ldap*）読み取り許可のみが割り当てられるためです。
>
> 次のコマンドを使用してパスフレーズを削除してください。
>
> openssl rsa -in server.enc.key.pem -out server.key.pem

4.4.7.3 OpenLDAP の設定

次の手順で OpenLDAP を設定します：

以下の手順は SuSE-YaST を元に記載されています。RedHat の場合は読み替えてください。

➢「Yast」セットアップツールを起動して、「LDAP」→「Server」→「Configuration」の順番で選択します。

➢「*Global Settings*/*Allow Settings*」の下で「*LDAPv2-Bind*」の設定を有効にしてください。

➢「*Global Settings*/*TLS Settings*」を選択します。

  ➢ TLS 設定を有効にします。

  ➢ インストール時に作成されたパスを宣言してください。（136 ページの「OpenLDAP のインストール」の節を参照してください。）

  ➢ ファイルシステムの証明書と秘密鍵が読み取ることができるのは、LDAP サービスのみであることを確認してください。

  「*openldap*」は「*uid/guid=ldap*」の下で実行されるので、以下のいずれかの方法となります。

  – ファイルのオーナーの証明書と秘密鍵を「ldap」に設定する、または、

  – LDAP デーモン、「*ldap*」の読み取り許可を証明書と秘密鍵が入ったファイルに割り当てる。

➢「*Databases*」を選択して新しいデータベースを作成します。

YaST で作成した設定が全く機能しない場合には、以下の必須エントリが次のファイルに存在しているかを確認してください。

/etc/openldap/slapd.conf:

allow bind_v2

TLSCACertificateFile /path/to/ca-certificate.pem

TLSCertificateFile /path/to/certificate.pem

TLSCertificateKeyFile /path/to/privat.key.pem

YaST で作成した SSL の設定が全く機能しない場合には、以下のエントリが設定ファイルに存在しているかを確認してください。

/etc/sysconfig/openldap:

OPENLDAP_START_LDAPS=“yes”

4.4.7.4 iRMC S2 ユーザー管理の OpenLDAP への統合

前提条件：

LDAP v1 もしくは、LDAP v2 ストラクチャが OpenLDAP ディレクトリサービスの中に生成済みであること。（90 ページの「SVS_LdapDeployer - 「SVS」と「iRMCgroups」ストラクチャの生成、保守および削除」の節を参照してください。）

iRMC S2 のユーザー管理の OpenLDAP の統合は以下の手順から成ります。

– iRMC プリンシパルユーザーの作成

– 新規 iRMC S2 ユーザーの作成とそのユーザーに対する許可グループの割り当て

プリンシパルユーザーを作成するには（ObjectClass :「Person」)、Jarek Gawor 氏著作の LDAP Browser\Editor などの LDAP ブラウザ（139 ページ参照）を使用します。

Jarek Gawor 氏の著作による LDAP Browser\Editor はグラフィカルユーザーインターフェースインターフェースによる使いやすいものです。

LDAP Browser/Editor は参考（推奨）として記載しています。LDAP Browser\Editor のインストール、及び仕様、設定に関する質問、お問い合わせはご遠慮願います。

このツールはインターネットからダウンロードにより入手できます。

以下の手順により **LDAP Browser\Editor** をインストールしてください。

➢ 圧縮アーカイブ「Browser281.zip」を任意のインストール用ディレクトリで解凍してください。

➢ JAVA のランタイム環境、たとえば、「JAVA_HOME=C:\Program Files\Jave\jdk1.5.0_06」用に環境変数「JAVA_HOME」をインストール用ディレクトリに設定してください。

JAVA_HOME=C:\Program Files\Jave\jdk1.5.0_06

プリンシパルユーザーの作成

プリンシパルユーザー（ObjectClass :「Person」)、Jarek Gawor 氏著作の LDAP Browser\Editor などの LDAP ブラウザ（139 ページ参照）を使用します。

以下の文章は、Jarek Gawor 氏の LDAP Browser\Editor を使用してプリンシパルユーザーを作成する方法を説明するものです。

以下の通り進めます :

- LDAP ブラウザを起動します。
- 有効な証明書データを使用して OpenLDAP ディレクトリサービスにログインしてください。
- プリンシパルユーザーを作成するサブツリー（サブグループ）を選択してください。
- プリンシパルユーザーはサブツリー内のどこにでも作成できます。
- 「Edit」メニューを開いてください。
- 「Add Entry」を選択します。
- 「Person」を選択します。
- 識別名 DN を編集します。

Active Directory のグループに「マニュアル」でユーザーを入力する必要があります。プリンシパルユーザーの識別名（DN）とパスワードは、対応する iRMC S2 の設定の項目に一致しなければなりません。(321 ページ、「ディレクトリサービス設定（LDAP）－ iRMC S2 のディレクトリサービスの設定」の節を参照してください。)

- ［Set］をクリックしてパスワードを入力してください。
- 苗字「SN」を入力してください。
- ［Apply］をクリックします。

新規 **iRMC S2** ユーザーの作成とそのユーザーに対する許可グループの割り当て

新規ユーザー（ObjectClass「Person」）を作成してそのユーザーに許可グループを割り当てるには、Jarek Gawor 氏の LDAP Browser\Editor などの LDAP ブラウザを使用します。（139 ページを参照してください。

以下の文章は、Jarek Gawor 氏の LDAP Browser\Editor を使用して新規の iRMC S2 ユーザーを作成し、そのユーザーに許可グループを割り当てる方法を説明するものです。

以下の通り進めます :

➢ LDAP ブラウザを起動します。

➢ 有効な証明書データを使用して OpenLDAP ディレクトリサービスにログインしてください。

➢ 新規ユーザーを作成します。

この作業は以下のように行います。

➢ 新規ユーザーを作成するサブツリー（サブグループ）を選択してください。

➢ 新規ユーザーはサブツリー内のどこにでも作成できます。

➢「Edit」メニューを開いてください。

➢「Add Entry」を選択します。

➢「Person」を選択します。

➢ 識別名「DN」を編集します。

➢［Set］をクリックしてパスワードを入力してください。

➢ 苗字「SN」を入力してください。

➢［Apply］をクリックします。

- 今作成したユーザーを許可グループに割り当てます。

  この作業は以下のように行います :

  - ユーザーを所属させる iRMCgroups または SVS サブツリー（サブグループ）を選択してください。すなわち、

  – *LDAP v1* の場合は。

    cn=UserKVM,ou=YourDepartment,ou=Departments,ou=iRMCgroups,

    dc=myorganisation,dc=mycompany

  – LDAP v2 の場合は。

    cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS,

    dc=myorganisation,dc=mycompany

- 「*Edit*」メニューを開いてください。
- 「*Add Attribute*」を選択します。
- 属性名として「*Member*」を指定します。変数にはここで作成したユーザーの完全修飾 DN を指定してください。すなわち、
- *cn=UserKVM,ou=YourDepartment,ou=Departments,ou=iRMCgroups,*
- *dc=myorganization,dc=mycompany*
- または
- cn=UserKVM,ou=YourDepartment,ou=Departments,ou=SVS,
- dc=myorganisation,dc=mycompany

4.4.7.5 OpenLDAP 管理のヒント

LDAP サービスの再起動

次の手順で LDAP サービスを再起動します：

- コマンドボックスを開きます。
- ルート権限でログインします。
- 次のコマンドを入力します。

  rcldap restart

メッセージログ作製

LDAP デーモンは 「*Syslog*」プロトコルを使用してメッセージログを作製します。

ログ化されたメッセージは次のファイルでログレベルが 0 に設定されている場合のみ表示されます。

/etc/openldap/slapd.conf.

各レベルの説明は以下を参照してください。

http://www.zytrax.com/books/ldap/ch6/#loglevel

144 ページの表 2 に、ログのレベルとその意味の概要をリストしています。

ログレベル	意味
-1	全面的なデバッグ実行
0	デバッグ実行なし
1	ログファンクションコール
2	試験パケットの取扱い
4	ヘビートレースデバッグ実行
8	接続管理
16	送信 / 受信パケット表示
32	フィルタ処理の検索
64	設定ファイル処理
128	アクセス管理リスト処理
256	接続／操作／イベントのステータスログ作成
512	送信したエントリのステータスログ作成
1024	シェルバックエンドによる出力通信
2048	エントリパースの出力結果

表 2： OpenLDAP - ログレベル

4.4.8 グローバル iRMC S2 ユーザー宛ての Email 警告の設定

グローバル iRMC S2 ユーザー宛の Email 警告は、グローバル iRMC S2 ユーザー管理に統合されています。すなわち、1 台のディレクトリサーバを使用してすべてのプラットフォームを集中的に設定し操作できます。適切に設定されたグローバルユーザー ID は、ネットワーク上でディレクトリサーバに接続されたすべての iRMC S2 から Email 警告を受け取ることができます。

前提条件：

Email 警告には以下の要点を満たす必要があります。

– グローバル Email 警告には、LDAP v2 のストラクチャとしてバージョン 3.77A 以降の iRMC S2 ファームウェアが必要です。

– プリンシパルユーザーは、iRMC S2 Web インターフェースに設定され LDAP ツリー内で検索できる許可を与えられている必要があります。（321 ページ、「ディレクトリサービス 設定（LDAP） – iRMC S2 のディレクトリサービスの設定」の節を参照してください。）

– ディレクトリサービス構成 ページ（321 ページ参照）上で LDAP を設定する際に、「ディレクトリサービス E-mail 警告構成」の下で Email 警告を使用可能にしておく必要があります。

4.4.8.1 グローバル Email 警告

ディレクトリサーバ経由の Email 警告には警告ロールが必要です。この警告ロールは管理ロールに加えて「SVS_LdapDeployer」（90 ページ参照）の設定ファイル内で定義されます。

警告グループ（警告ロール）の表示

警告ロールは警告タイプ（たとえば、温度のしきい値を超えた、など）をまとめてグループ化しますが、それぞれに Severity（たとえば「致命的」）が割り当てられています。ユーザーを特定の警告グループに割り当てると、ユーザーが Email で受ける警告のタイプと重大度が指定されます。

警告ロールの構文はサンプル設定ファイル、「*Generic_Settings.xml*」および

「*Generic_InitialDeploy.xml*」によって解説されます。サンプルファイルは ServerView Suite の DVD1 の中の「jar」アーカイブ、「*SVS_LdapDeployer.jar*」にあります。

警告タイプの表示

以下の警告タイプがサポートされます :

警告タイプ	原因
FanSens	冷却ファンセンサー
Temperat	温度センサ
HWError	致命的なハードウェア故障
Security	セキュリティ
SysHang	システムのハング
POSTErr	POST エラー
SysStat	システムステータス
DDCtrl	ディスクドライブとコントローラ
NetInterf	ネットワークインターフェース
RemMgmt	リモートマネジメント
SysPwr	電源管理
Memory	メモリ
Others	そのほか

表 3： 警告タイプ

各々の警告タイプには以下の重大度のいずれかが割り当てられます。
警告、致命的、すべて、(なし)

優先メールサーバ
グローバル Email 警告には、優先メールサーバの「Automatic」設定が適用されます。Email が即時に送ることができない場合、たとえば 1 番目のメールサーバが使用不可能な場合には、Email は 2 番目のメールサーバに送られます。

サポートされるメールフォーマット

以下の Email フォーマットがサポートされます。

– 標準
– Fixed Subject
– ITS- フォーマット
– 富士通 REMCS フォーマット

標準以外のメールフォーマットが使用される場合は、ユーザーに対応するメールフォーマットグループを追加しなければなりません。

LDAP メールテーブル

Email 警告 (149 ページ参照) が設定され、オプションの「LDAP Email Alert Enable」(321 ページ参照) が選択された場合は、iRMC S2 は警告が発信された場合に以下のユーザーに Email を送信します。

– 適切に設定されたすべてのローカル iRMC S2 users、

– その警告用の 「LDAP Email」テーブルに登録されたすべてのグローバル iRMC S2 ユーザー。

LDAP Email テーブルは、iRMC S2 が初回に起動されたときに、iRMC S2 ファームウェアにより最初に作成され、定期的に更新されます。LDAP Email テーブルのサイズは、最大 64 の LDAP 警告ロールと最大 64 の Email 警告が設定された iRMC S2 ユーザーに限定されます。

グローバル Email 警告には Email 配布リストの使用を推奨します。

LDAP ディレクトリサーバは、Email 警告の目的で、以下の情報を Email テーブルから取得します :

- Email 警告が設定されたグローバル iRMC S2 ユーザーのリスト
- 各々の iRMC S2 ユーザーには、
  - 警告タイプ毎に設定された警告のリスト（タイプと重大度）
  - 要求されたメールフォーマット

「LDAP Email」テーブルは以下の環境で更新されます :

- iRMC S2 初回に起動または再起動されたとき、
- LDAP 設定が変更されたとき、
- 定期的（オプション）。更新の間隔は、iRMC S2 Web インターフェースの LDAP 設定の一部として（「LDAP 警告テーブルを更新する」オプション）指定します。（321 ページの「ディレクトリ サービス設定（LDAP） – iRMC S2 のディレクトリサービスの設定」の節を参照してください。

ディレクトリサーバ上のグローバル Email 警告の設定

この節ではディレクトリサーバ上に LDAP Email 警告を設定する方法を説明します。

設定は、iRMC S2 上にも行う必要があります。これらは、iRMC S2 Web インターフェース上で、設定します。（321 ページ、「ディレクトリサービス設定（LDAP） – iRMC S2 のディレクトリサービスの設定」の節を参照してください。）

以下の通り進めます：

➢ ディレクトリサービスに Email 警告を送信するユーザーの Email アドレスを入力します。

Email アドレス設定に使用する方法は、運用するディレクトリサービス（Active Directory または OpenLDAP）によって異なります。

➢ 警告ロールと定義する設定ファイルを作成してください。

➢ この設定ファイルを使用する「*SVS_LdapDeployer*」を起動し、対応する LDAP v2 ストラクチャ（SVS）をディレクトリサーバ上に生成させてください。（91 ページと 99 ページを参照してください。）

4.4.8.2 警告ロールの表示

LDAP v2 ストラクチャが生成されると、新たに作成された OU「SVS」が Active Directory に表示されます。たとえば、「*Declarations*」の配下の「*Alert Roles*」と「*Alert Types*」コンポーネントと一緒に、および、「*DeptX*」の配下の「Alert Roles」コンポーネントと一緒に表示されます：(図 50 を参照してください。)

– 「Declarations」の下に「Alert Roles」に定義された警告ロールが表示され、すべての警告タイプは「Alert Types」の下に表示されます。(1)

– DeptX の配下の Alert Roles に OU DeptX に有効な警告ロールがすべて表示されます。(2)

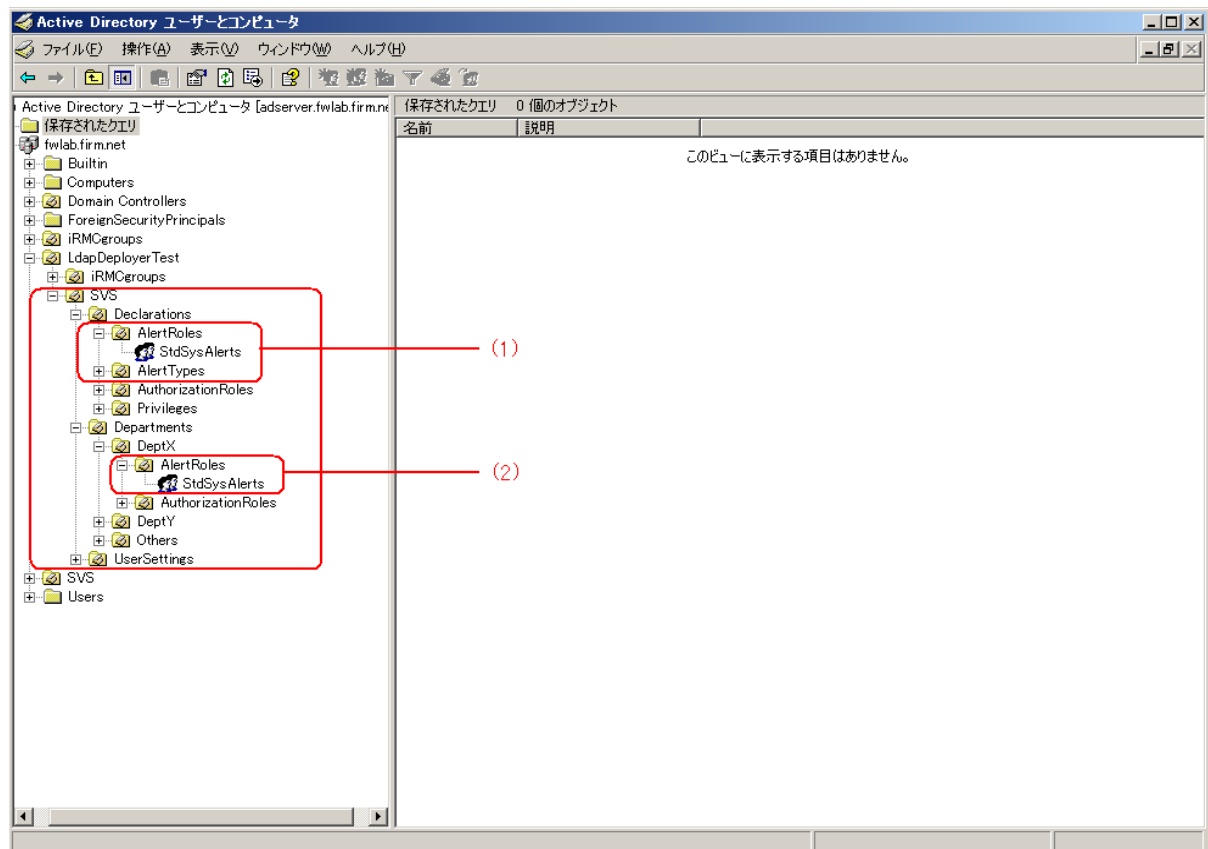



図 50：OU SVS と警告ロール

個々の警告ロールのユーザーに Email が送信されたことを確認するために、関連部門を iRMC S2 に設定する必要があります。(図 50 中の「*DeptX*」)(325 ページ参照を参照してください。

「***Active Directory*** ユーザーとコンピュータ」のストラクチャツリーで「***SVS***」-「***Departments***」-「***DeptX***」-「***Alert Roles***」の下にある警告ロール（たとえば、「***StdSysAlerts***」）を選択し（図 **51** 参照）（**1**）、コンテキストメニューから「プロパティ」-「メンバ」を選択することにより「プロパティ」ダイアログボックスを開いたとすると、その警告ロール（この例では「***StdSysAlerts***」）が「メンバ」タブの中に表示されます（**2**）。

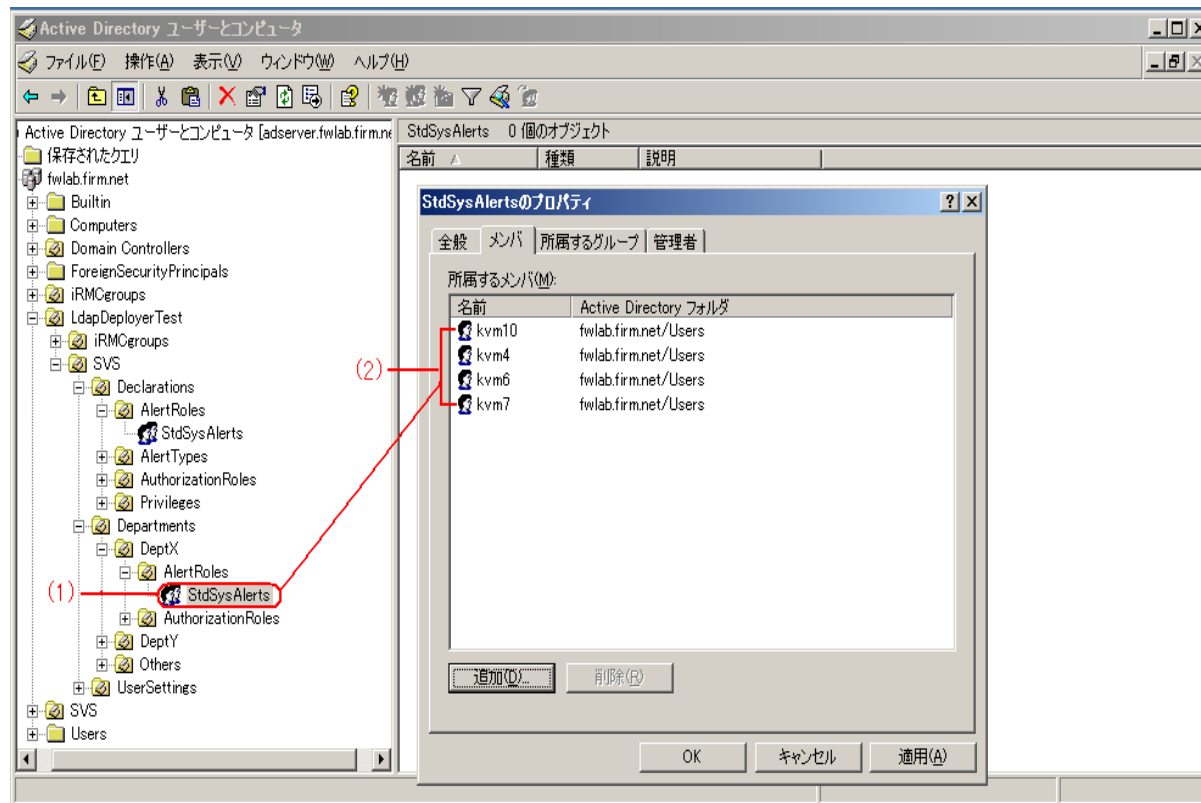



図 **51**: 警告ロール「**StdSysAlert**」に割り当てられたユーザー

4.4.8.3 iRMC S2 ユーザーへの警告ロール割り当て

iRMC S2 ユーザーに警告ロールを以下のいずれかの方法で割り当てる事ができます。

- ユーザーエントリに基づいて、または、
- ロールエントリに基づいて。

ことなる種類のさまざまなディレクトリサービス（**Microsoft Active Directory** および **OpenLDAP**）の中で、**iRMC S2** のユーザーが **iRMC S2** の承認ロールに割り当てられるのと同じ方法で、同じツールを使用して、**iRMC S2** ユーザーは、**iRMC S2** 警告ロールに割り当てられます。

たとえば、**Active Directory** の中では、「**Active Directory** ユーザーとコンピュータ」スナップインの「プロパティ」ダイアログボックスの中の「追加」をクリックして割り当てを行います。（図 51 を参照してください。）

4.4.9 SSL copyright

iRMC S2-LDAP の統合には、**OpenSSL** プロジェクトに基づき、**Eric Young** 氏が開発した **SSL** 実装を使用します。

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

5 章 ビデオリダイレクション（AVR）

ビデオリダイレクション機能を使用するには有効なライセンスキーが必要です。

ビデオリダイレクション（**AVR**）を使用すると、管理対象管理対象サーバのマウスとキーボードをリモートの管理端末から操作することができ、管理対象サーバの現在のグラフィック画面とテキスト出力を表示させることができます。

AVR Java アプレットを使用するとリモートストレージ機能も使用できます。（180 ページ、「リモートストレージ」の章を参照してください。）

本章では次の点について説明します：

- **AVR** 設定の確認
- **AVR** の使用
- **AVR** ウィンドウのメニュー

5.1 要求事項：AVR 設定の確認

AVR を使用する前に以下の重要な設定を確認してください。

管理対象サーバ上のグラフィックモード設定

AVR は下記のグラフィックモードをサポートします：

解像度	リフレッシュレート［**Hz**］	最大色深度［ビット］
640 x 480 (VGA)	60; 75; 85	32
800 x 600 (SVGA)	56; 60; 72; 75; 85	32
1024 x 768 (XGA)	60; 70; 75; 85	32
1152 x 864	60; 70; 75	32
1280 x 1024 (UXGA)	60; 70; 75; 85	16
1280 x 1024 (UXGA)	60	24
1600 x 1200 (UXGA)	60; 65	16

表 4： サポート可能なディスプレイ設定

i サーバに高解像度のグラフィックモードが設定されている場合（表中で背景色がグレイになっているもの）は、「iRMC Web」インターフェース上で表示されます。

i サポートされるのは VESA 準拠のグラフィックモードのみです。

サポートされるテキストモード

iRMC S2 は下記の共通テキストモードをサポートします。

– 40 x 25

– 80 x 25

– 80 x 43

– 80 x 50

ディスプレイ設定の情報はお使いの OS のヘルプ画面から参照してください。

キーボード設定

以下のキーボード設定は同一でなければなりません。

- リモート管理端末上

- 管理対象サーバ上

– iRMC S2 上

5.2 AVR の使用方法

➢ AVR を起動させるには、iRMC S2 Web インターフェース上の「*Advanced Video Redirection (AVR)*」ページの［ *Start Video Redirection* ］または［*Start Video Redirection (Java Web Start)* ］ボタンをクリックしてください。(321 ページを参照してください。)

「*Advanced Video Redirection*」ウィンドウ（AVR ウィンドウ）が開き、管理対象サーバ上のディスプレイが表示されます。

AVR ウィンドウには以下の要素も含まれています。

- メニューバー :「*Preferences*」および「Extras」メニューにより、AVR 設定しコントロールすることができます。(172 ページを参照してください。)「*Remote Storage*」はリモートストレー ジ機能の呼び出しに使用します。(162 ページを参照してください。

  「*Languages* 」メニュー（162 ページ参照）を使用すると、AVR ウィンドウのメニューとダイアログボックスに表示される言語（ドイツ語／英語）を設定できます。
- 統合された特殊キー（162 ページを参照してください）。
- 「*Local Monitor <status>* 」インディケータは管理対象サーバのサーバ側モニタの電源ががオンになっているかどうかを表示します。(161 ページ、「サーバ側のモニタ ON/OFF 機能」の節を参照してください。)

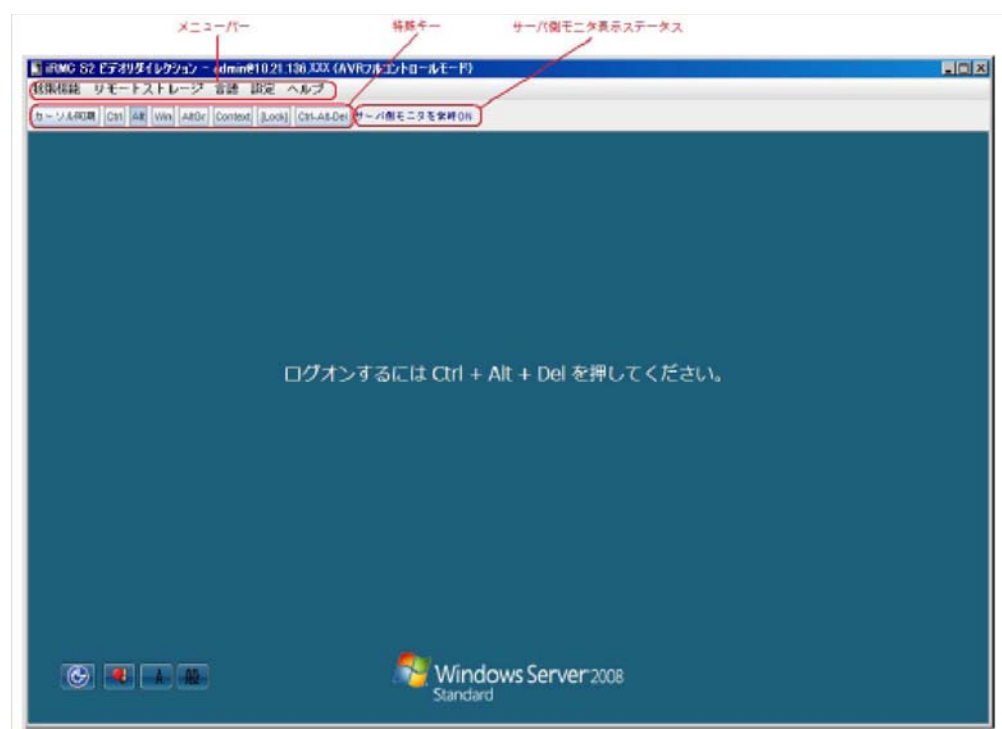



図 52 : アドバンストビデオリダイレクション（AVR）ウィンドウ

5.2.1 AVR の複数接続

AVR は 2 つのユーザーセッションを同時に行うことができます。一方のユーザーはサーバをフルコントロールでき（フルコントロールモード）、他方のユーザーはサーバのキーボードとマウス操作を監視すること（ビューモード）ができます。

AVR を初めて起動すると最初にビューモードとなります。その後、フルコントロールモードに切り替えるかどうかが必ず尋ねられます。フルコントロールモードへ切り替えることを決定したときに、他にフルコントロールモードが使用されている場合には、そのセッションはビューモードに切り替えられます。

5.2.2 サーバ側のモニタ ON/OFF 機能

iRMC S2 の「Local Monitor Off」機能により、AVR セッションを行う間管理対象サーバのサーバ側モニタの電源をオフにすることができます。この方法により、AVR を使用してサーバ側モニタ上で行ったインプットや実行した処理を見られることはありません。 識別用 LED が点滅してサーバが「サー バ側モニタ ON ／ OFF」モードであることを示します。

「サーバ側モニタ ON ／ OFF」機能は、iRMC S2 Web インターフェースの「*Advanced Video Redirection*」ページから設定することができます（344 ページを参照してください。）システムを適切に設定したら、リモートの管理端末からサーバのサーバ側モニタを以下のようにオンオフできます。

- Extras メニューを使用するフルコントロールモードから
- 管理者または OEM の権限により、直接「*Advanced Video Redirection*」から

新たに AVR セッションが開始されたときには、必ずサーバ側モニタを自動的にスイッチオフにする設定をすることもできます。

サーバ側モニタの現在の状態は、AVR ウィンドウで、統合された特殊キーの右上に青地で表示されます：

サーバ側モニタが常時オン

サーバ側モニタは、「Enable Local Monitor Off」オプション（349 ページ参照）が無効にされるので、サーバ側モニタは、常時スイッチオン状態でオフにすることはできません。

サーバ側モニタオン

サーバ側モニタはオンになっていますがスイッチオフできます。

サーバ側モニタオフ

サーバ側モニタはオフになっていますがスイッチオンできます。

サーバ側モニタが常時オフ

サーバ側モニタは常時スイッチオフで、スイッチオンにはできません。管理対象サーバ上で高解像度のグラフィックモードが設定されているためです。（表 4 を参照してください。）

5.2.3 キーボードのリダイレクション

キーボードのリダイレクションは AVR ウィンドウにフォーカスされている場合のみ可能です。

- キーボードのリダイレクションが機能していない場合にはまず AVR でクリックしてください。
- キーボードの反応がない場合は、AVR ウィンドウがビューモードになっていないかどうかを確認してください。フルコントロールモードに切り替える方法は、78 ページに説明があります。

特殊キーの組合せ

AVR は通常のキーの組合せはすべてサーバに伝えられます。 ウィンドウズキーなどの特殊キーは伝送されません。[ALT] + [F4] などの一部の特殊キーの組合せは伝送できません。クライアントのオペレーティングシステムにより中断されるからです。このような場合は、特殊キーの同時使用またはグラフィカルキーボードを使用してください。

統合された特殊キー

AVR ウィンドウのメニューバーの下に、特殊キーのバーがあります。これらのキーは「スティックキー」として機能します。すなわちクリックすると押したままの状態が続き、もう一度クリックするとまた元の位置に戻ります。

統合された特殊キーを使用すると、たとえば、キーボード上で押しても AVR に伝送されないウィンドウズキーや特殊キーの組合せを使用することができます。

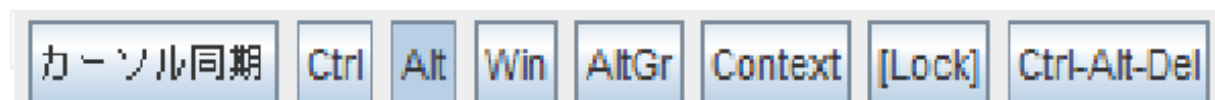



図 53： **AVR** ウィンドウ – 統合された特殊キー

［カーソル同期］

このキーを押してマウスポインタを同期させます。（合わせて 164 ページ、「マウスポイン タの同期」の節を参照してください。）

［Ctrl］

左の CTRL キー（キーボードの［Ctrl］キーに相当します）。

［Alt］

Alt（ernate）キー（キーボードの［Alt］キーに相当します）。

［Win］
　左右のウィンドウズキー（キーボードの左右の［Ctrl］キーと［Alt ］キーの間にあるキーに相当します）。

［Alt Gr］
　Alt（ernate）Graphic）キー（キーボードの［Alt Gr］キーに相当します）。

［Context］
　選択したメニューのコンテキストメニューです（キーボードの［Shift］＋［F10］キーの組合せに相当します）。

［Lock］
　Caps lock キー（キーボードの［Caps Lock］キーに相当します）。

［Ctrl-Alt-Del］
　キーボードの［Ctrl］＋ ［Alt］＋ ［Del］の組合せに相当します。

グラフィカルキーボード

グラフィカルキーボード（図 54 参照）はキーボードを代替する機能があります。グラフィカルキーボードを使用するとすべてのキーの組合せを使用できます。すなわち、グラフィカルキーボードでは実際のキーボードを完全に代替する機能が使用可能です。

グラフィカルキーボードは「Extras」メニュー（173 ページ参照）から起動できます。

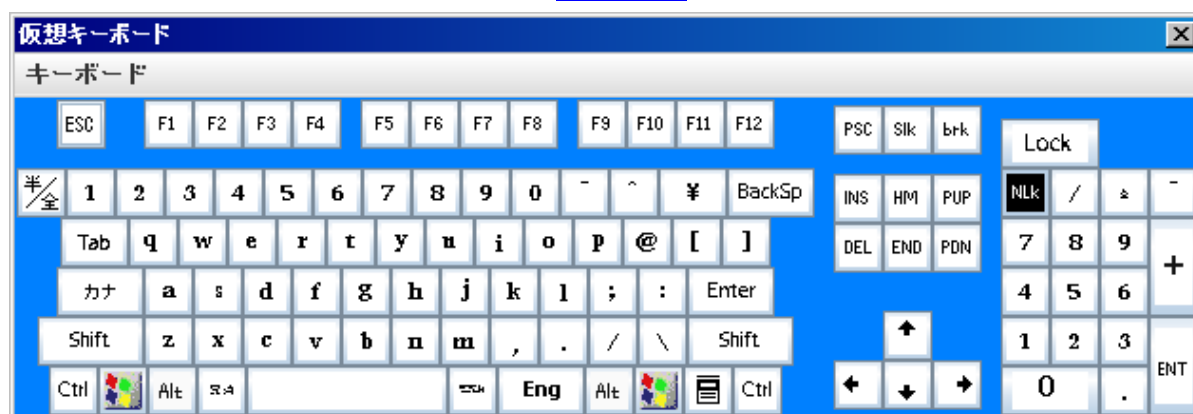



図 54： グラフィカルキーボード（日本語レイアウト（JP））

セキュアキーボード

iRMC S2 Web インターフェースを HTTPS 接続している場合は、キーボードの入力は、セキュア SSL 接続により伝送されます。

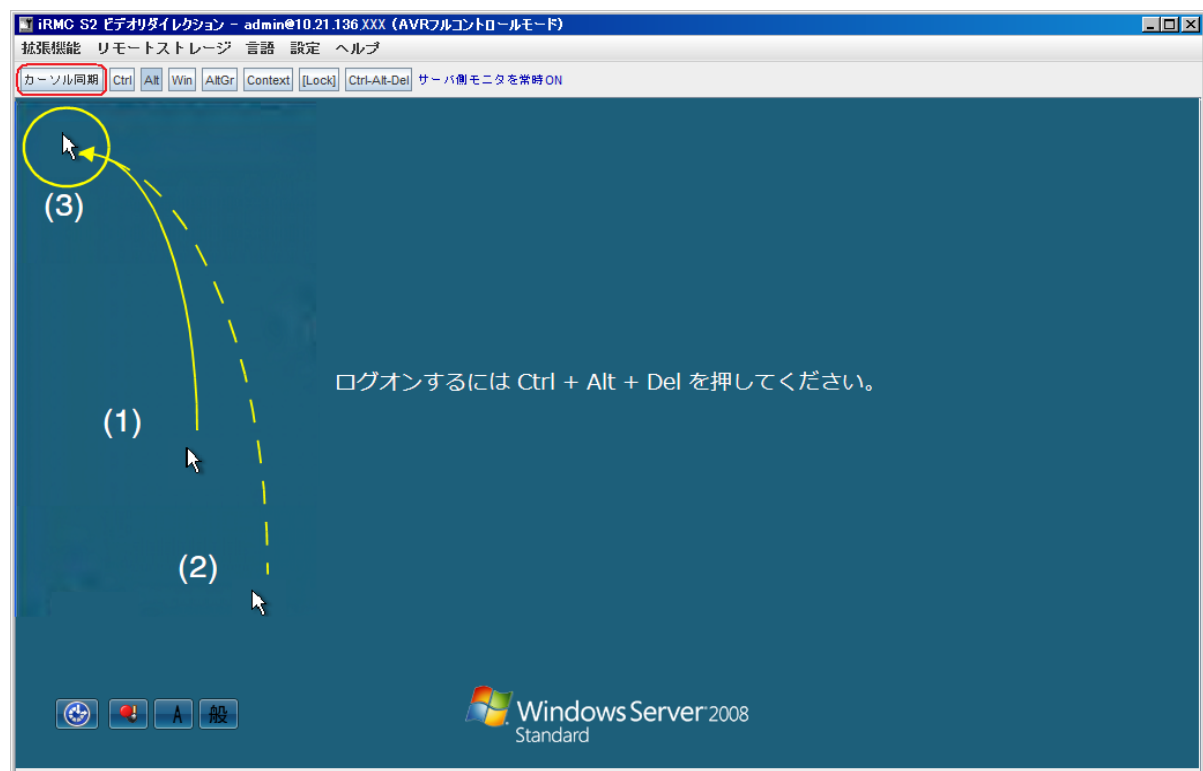
5.2.4 マウスのリダイレクト

管理対象サーバのマウスポインタは、リモート管理端末のマウスに同期して動かすことができます。マウスのリダイレクション設定は、**AVR** ウィンドウで「***Preferences***」メニュー（177 ページ参照）の「**Mouse**」タブから設定します。

5.2.4.1 マウスポインタの同期

AVR ウィンドウを最初に開いたときには、リモート管理端末のマウスポインタ（サーバ側マウスポインタ）はまだ管理対象サーバのマウスポインタに同期していないこともあります。

両方のマウスポインタを以下のいずれかの方法で同期させてください。（図 55 を参照してください。）：

- ➢ **AVR** ウィンドウ、メニューバーの［カーソル同期］をクリックしてください。
- ➢ サーバ側マウスポインタを AVR ウィンドウの左上隅まで動かす。管理対象サーバのマウスポインタは自動的にこの動きに追随します。
  両方のマウスが完全に重なればにポインタは同期します。

カーソル同期ボタンを押下する。

又は
（1）操作側のマウスカーソルを画面左上に移動する。
（2）サーバのマウスカーソルも自動的に同じ場所へ移動する。
（3）操作側とサーバのマウスカーソルが重なり、シンクロ動作が開始される。

図 55： サーバ側マウスポインタと管理対象サーバのマウスポインタの同期化

i マウスポインタを正常に同期させるには、管理対象サーバ側で特定の設定を行う必要があります。管理対象サーバが「**ServerView Installation Manager**」を使ってインストールされていれば、この設定は **Matrox VGA** インストレーションによって自動的に初期設定されています。

i マウスポインタの同期が正常に機能しない場合、たとえば初期設定が変更されている 場合には、以下に説明する設定を行えば正常なマウスポインタの同期に戻すことができます。この設定は管理対象サーバ側で行う必要があります。

5.2.4.2 管理対象 Windows サーバ：マウスポインタ同期設定の調整

Windows サーバの場合は、マウスポインタ同期の設定はバッチファイルを使用する方法か、**Windows** スタートメニューとコンテキストメニューを使用する方法のいずれかで行うことができます。

次の設定を調整してください。

- マウスポインタの速度
- ハードウェアアクセラレーション

バッチプログラムを使用して設定の調整を行う場合は、調整するマウスポインタの速度やハードウェアアクセラレーション用のドライバのみでなく **Matrox** のグラフィックドライバをインストールします。

管理対象サーバの設定は、直接管理対象サーバでもできますが、**AVR** を使用してリモートの管理端末から行うこともできます。

バッチプログラムを使用する管理対象サーバ設定の調整

以下の通り進めます：

➢ コマンドプロンプトウィンドウを開きます。

➢ 関連する **Matrox VGA** ドライバインストール（**32** ビットまたは 64 ビット）用のバッチプログラム **install_kronos2_vga.bat** があるフォルダに切り替えます。

デフォルト設定では **install_kronos2_vga.bat** プログラムは：

C:¥Program Files¥Fujitsu¥ServerView Suite¥Installation Manager¥ Content¥V10.09.12.00¥DRV¥VIDEO¥MATROX¥iRMC¥W2K

の下にあります。また、「**ServerView Suite**」の **DVD 1** にも入っています。

➢「**setup.bat**」とタイプしてバッチプログラムを起動してください。

➢ バッチプログラムが実行されたら、管理対象サーバをリブートします。

Windows スタートメニューとコンテキストメニュー使用する管理対象サーバ設定の調整

以下の手順でマウスポインタを調整します：

➢ 次の通り選択します。

「スタート」→ 「設定」→「コントロールパネル」→「マウス」

さらに「ポインタ オプション」タブを選択します。

その結果以下のウィンドウが開かれます。

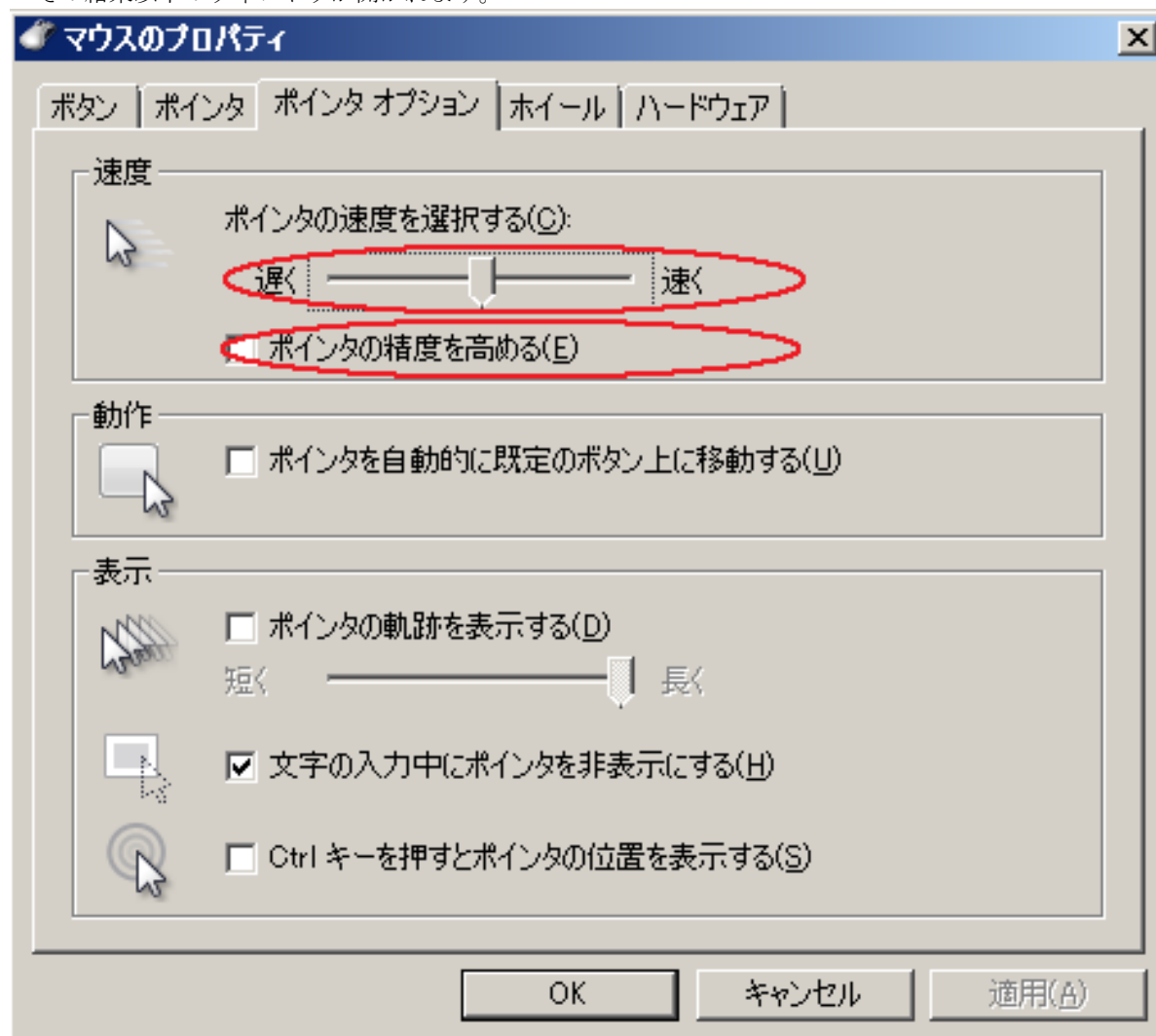



図 56: マウスプロパティウィザード、ポインターオプションタブ

➢ 「ポインタの速度を選択する」は中位の値に設定します。

➢ 「ポインタの制度を高める 」オプションは無効にします。

➢ [OK] ボタンをクリックして設定をセーブします。

以下の手順でハードウェアアクセラレータを調整します。

- デスクトップの背景を右クリックします。
- 現れたコンテキストメニューから、次のように選択します。

「設定」タブ、[詳細設定] ボタン、続いて「トラブルシューティング」タブその結果以下のウィンドウが開かれます。

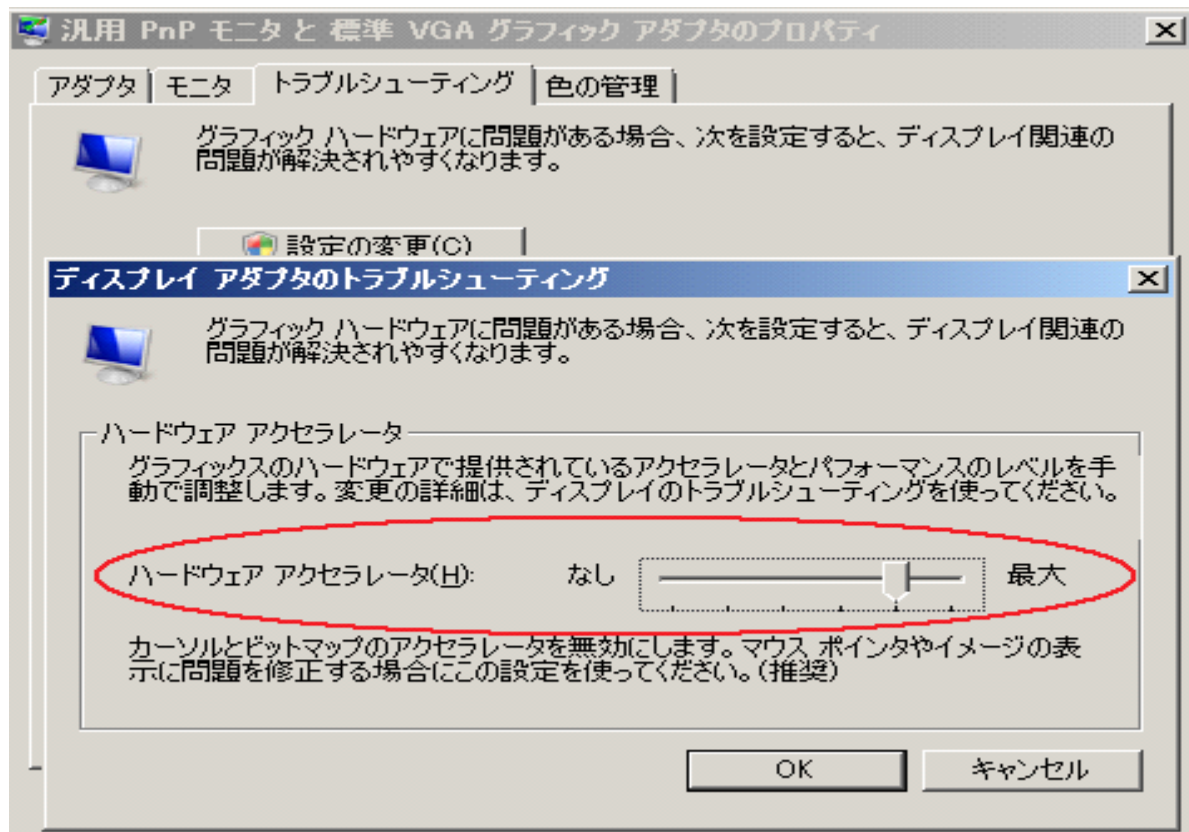



図 57: プロパティ トラブルシューティング : - ハードウェアアクセラレータ

- 「ハードウェアアクセラレータ」を図 57 で示された値に設定してください。
- [OK] ボタンをクリックして設定をセーブします。

5.2.4.3 管理対象 **Linux** サーバ：マウスポインタ同期設定の調整

前提条件　管理対象サーバは以下の **Linux** オペレーティングシステムのいずれかが稼働していることが前提となります。

- **Red Hat 4.x**
- **Red Hat 5.x**

Redhat Linux では異なるグラフィカルユーザーインターフェース (**GUI**) を使用することができます。最も重要な **GUI** を以下に示します。

- **Gnome**
- **KDE**

管理対象サーバのマウスポインタの同期設定は、コマンドを使用するかメニューのガイドに従うかして調整することができます。

次の設定を調整してください。

- ***Mouse motion acceleration = 1***
- ***Mouse motion threshold =1***

管理対象サーバの設定は、直接管理対象サーバでもできますが、AVR を使用してリモートの管理端末から行うこともできます。

管理対象サーバ仮設定のコマンドによる調整

「*xset*」コマンドを使用して「**Pointer acceleration**」と「**Pointer threshold**」の今回のセッションの間使用する設定をします。（推奨値はどちらも 1 です。）

コマンドのシンタックス

xset m(ouse)][*acceleration*][*threshold*]

以下の通り進めます。

- コマンドラインツールを呼び出します。
- 「**xset**」コマンドを以下の引数で実行します。

xset m 1 1

設定ファイル (KDE) による管理対象サーバの永久設定の調整

以下の通り **KDE** の永久設定を行います。

➢ テキストファイル **/root/.kde/share/config/kcminputrc** の設定を以下のように変更します。

[Mouse]
Acceleration=1
Threshold =1

サーバをリブートした後に数値を設定し直す必要はありません。

メニューガイドによる管理対象サーバの永久設定の調整

サーバを再起動した後に数値を設定し直す必要はありません。

以下の通り **KDE** の永久設定を行います。

以下に説明する **KDE** の手順は **SuSE Linux** のみに適用されます。
SuSE Linux は未サポートです。

➢ 以下の順序で選択します。
「***N***」→「***Control Center***」→「***Peripheral*** 」→「**Mouse - Advanced**」タブ
「***Mouse - Control Center***」ウィンドウが開きます。

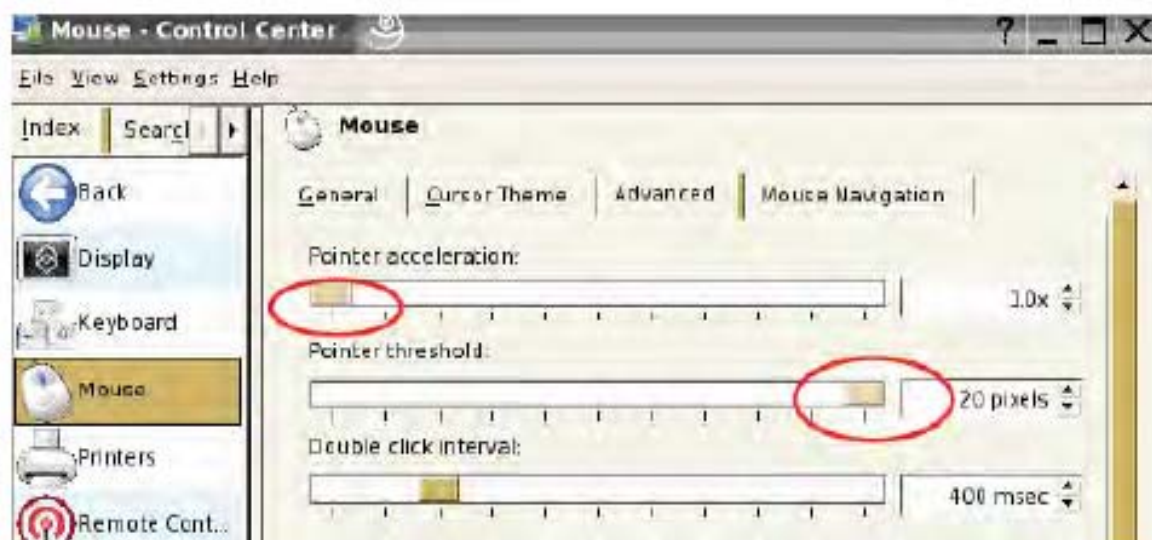



図 58: マウスコントロールセンターウィンドウ

➤ **Mouse Control Center** ウィンドウで下記の数値を設定します。

- 「**Pointer acceleration: 1.0x** 」（最小値）
- 「**Pointer threshold: 20** ピクセル」（最大値）

➤ 設定をセーブします。

➤ 管理対象サーバをリブートします。

サーバを再起動した後に数値を設定し直す必要はありません。

以下の通り **Gnome** の永久設定を行います。

➤ シェルの中から「**gconf-editor**」エディタを呼び出します。

➤「**desktop**」→「**gnome**」→「**peripherals**」→「**mouse**」

➤ 次の属性変数を変更します。

motion_acceleration 1

motion_threshold 1

5.3 AVR ウィンドウのメニュー

AVR ウィンドウのメニューバーには以下のメニューがあります。

- 「拡張機能」メニューを使用して **AVR** セッションのコントロールができます。グラフィカルキーボードを使用可能にすることもできます。
- 「リモートストレージ」メニューを使用してリモートストレージ接続の設定と解除ができます。
- 「言語」メニューでは「**AVR**」メニューとダイアログ表示に使用する言語（ドイツ語、英語または日本語）の設定ができます。
- 「設定」メニューはマウス、キーボード、および、ログイン設定の設定ができます。

5.3.1 Extras メニュー

「拡張機能」メニューから以下の機能を選択できます。

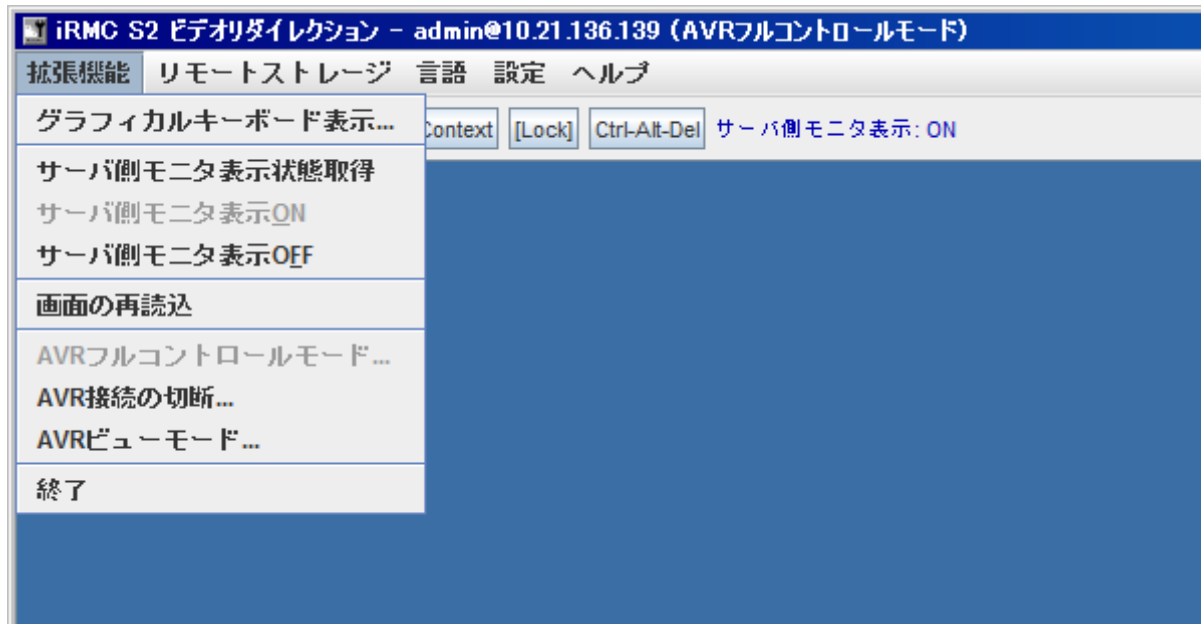



図 59: **AVR** ウィンドウ – 「拡張機能」メニュー

「キーボード」

グラフィカルキーボードが開きます。(図 54 を参照してください。)

「サーバ側モニタ状態を更新」

サーバ側モニタ状態の表示をリフレッシュします。

「サーバ側モニタ表示 ***ON***」

管理対象サーバのサーバ側モニタ出力を有効にします。

i サーバ側モニタの出力が **OFF** されていても、以下のケースではこの機能は使用できなくなります。

- - ビューモードにあるとき、
- - 管理対象サーバに高解像度のグラフィックモードが設定されている場合(157 ページの表 4 を参照してください)。

サーバ側モニタ<状態>表示

サーバ側モニタを常時 ***OFF***

サーバ側モニタ出力 ***OFF***

管理対象サーバのサーバ側モニタ出力を無効にします。

サーバ側モニタの出力が **ON** されていても、以下のケースではこの機能は使用できなくなります。

- ビューモードにあるとき、
- **AVR** を起動したときに、「サーバ側モニタ出力 **OFF**」オプションがサーバ側モニタで有効になっていない場合。(348 ページを参照してください。)

  サーバ側モニタ＜状態＞表示

  サーバ側モニタを常時 **ON**

「画面リフレッシュ」

AVR ウィンドウをリフレッシュします。

「フルコントロールへ変更」

AVR フルコントロールモードに切り替えます。(すでにフルコントロールモードになっている場合はこの機能は使用できません。)

次のダイアログボックスが開きます。

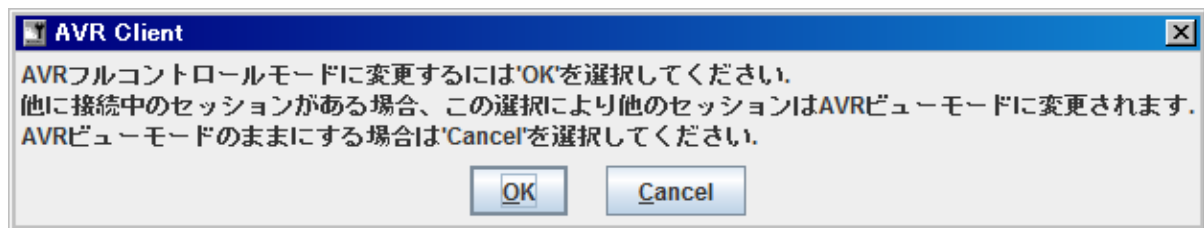



図 60:「機能拡張」メニュー - **AVR** フルコントロールへ変更

➢ [*OK*] をクリックして **AVR** フルコントロールモードへの切り替えを確定します。

すでに開いている **AVR** フルコントロールのセッションはビューモードに切り替わりますので注意してください。

➢**AVR** フルコントロールモードへ切り替えたくない場合には［***Cancel***］をクリックします。

「セッション切断……..」

別の AVR セッションを終了させます。

「セッション切断」で終了させることができるの別の AVR セッションのみです。

現在のセッションを終了させるには「Exit」を選択します。

現在の AVR セッションのリストが表示されます。

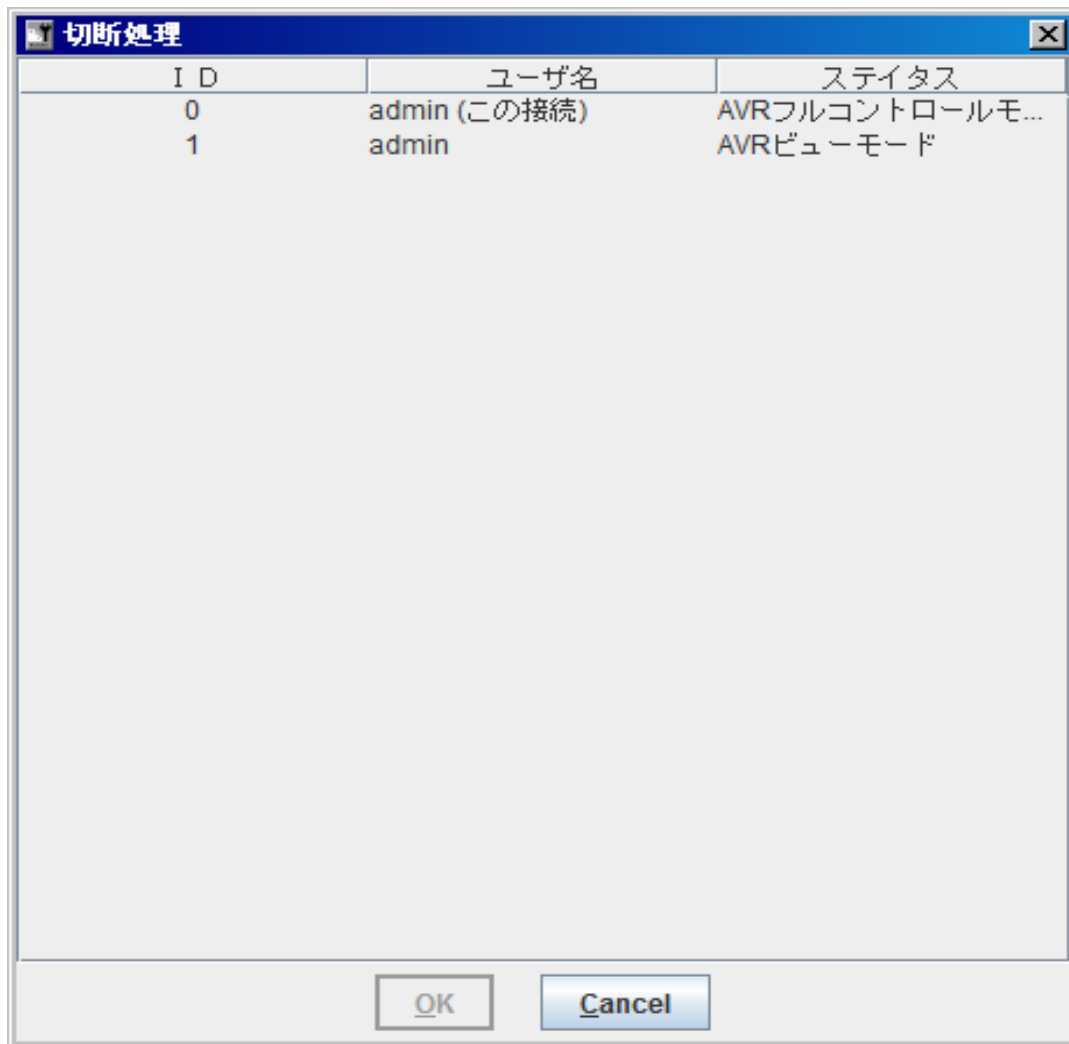



図 61 :「拡張機能」メニュー － セッションの切断

- 終了させたい「AVR」セッションを選択します。
- [OK] をクリックして選択した AVR セッションの終了を確定します。
- 選択した「AVR」セッションを終了させたくない場合は [Cancel] をクリックしてください。

「*AVR* ビューモード」

ビューモードに切り替えます。（すでにビューモードになっている場合はこの機能は使用できません。）

「終了」

現在の「AVR」セッションを終了させます。

5.3.2 リモートストレージメニュー

「リモートストレージ」の下の「リモートストレージ」機能を呼び出します。

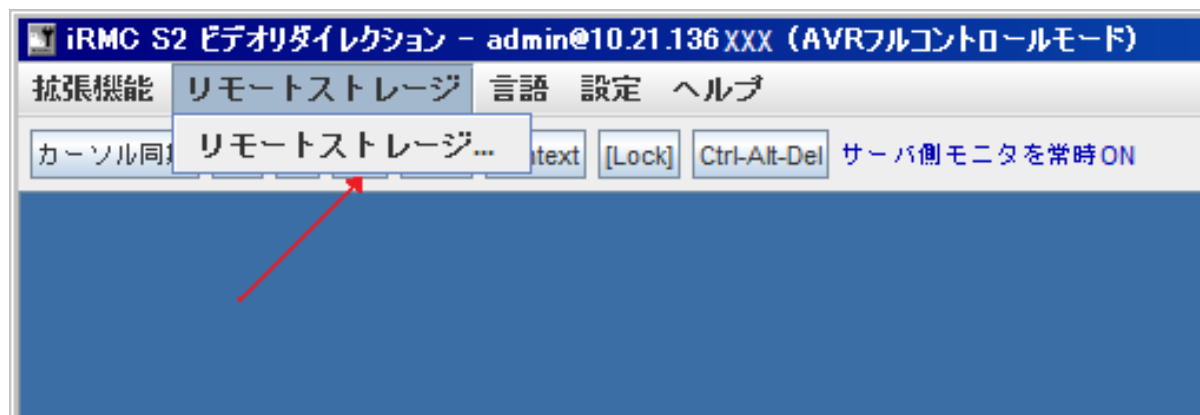



図 62： AVR ウィンドウ –「リモートストレージ」メニュー

リモートストレージ

「リモートストレージ…」をダブルクリックすると「ストレージデバイス」ウィンドウが開きます（183 ページを参照してください。）このウィンドウを使用してリモートストレージとしてリモート管理端末にメディアを取り付けまたは取り外すことができます。（180 ページ、「リモートストレージ」の章を参照してください。）

5.3.3 言語メニュー

「言語」メニューから AVR ウィンドウのメニューとダイアログの表示に使用する言語を選択します。

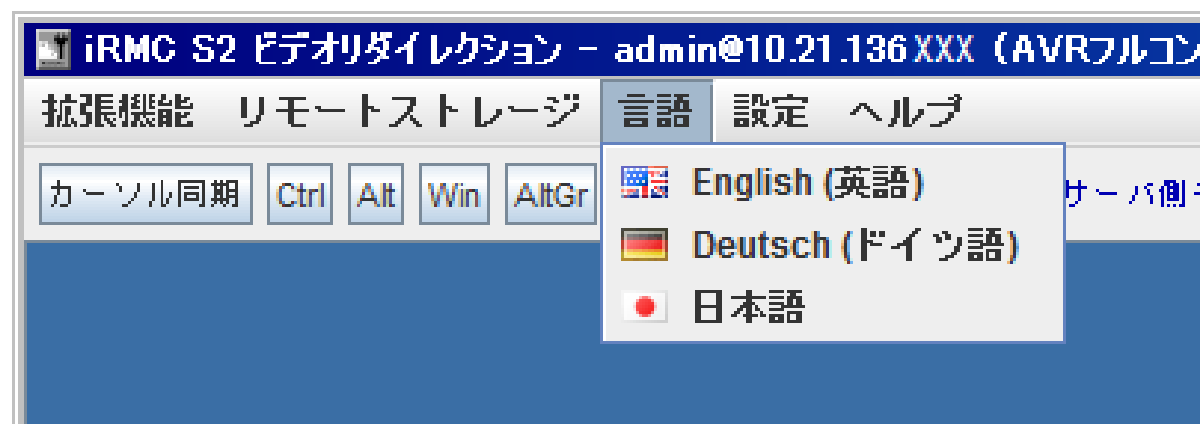



図 63： AVR ウィンドウ – 言語 メニュー

5.3.4 設定メニュー

「パフォーマンス設定」メニューには、マウス、キーボード、ログインの設定を行うそれぞれのタブがあり、その他の機能に使用する「その他設定」タブと合わせて使用します。

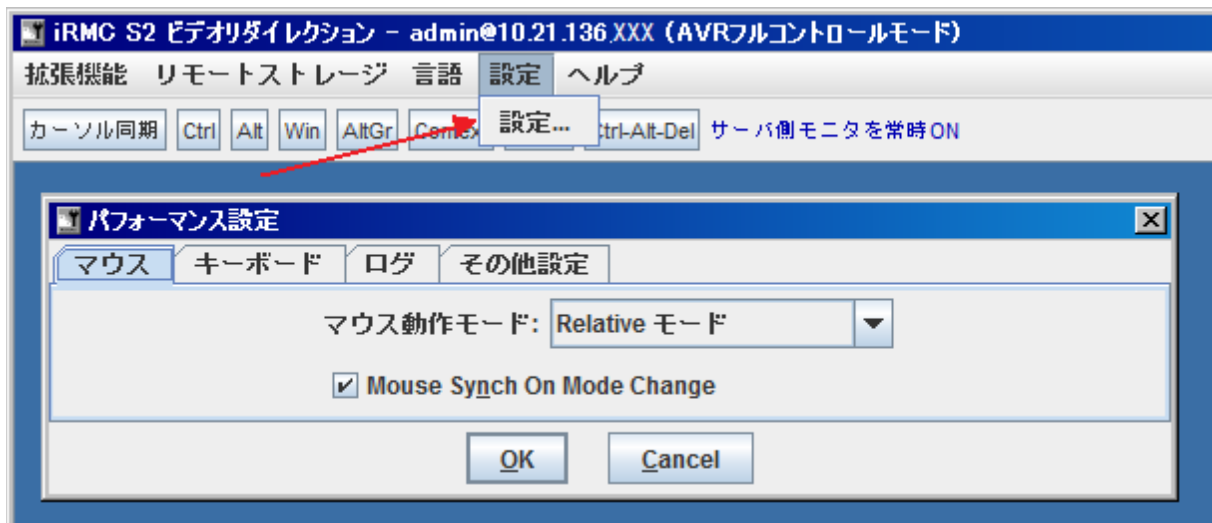



図 64： 「AVR ウィンドウ」－ 「パフォーマンス設定」メニュー
マウスタブ

「マウス」タブでマウスのモードを指定することができます。

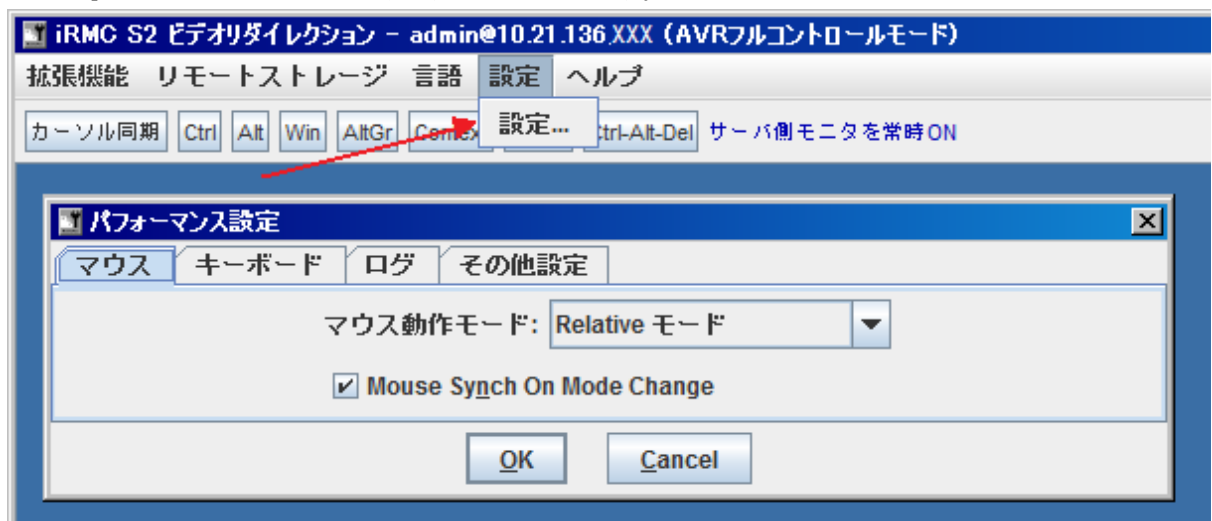



図 65 :「パフォーマンス設定」メニュー－「マウス」タブ

サーバのオペレーティングシステムごとに以下の設定が必要になります。

- Windows : Absolute モード、操作側を非表示 (Relative) または Relative モード
- Linux : 操作側を非表示（Relative）または Relative もーど

初期設定 : *Relative* モード

➤ 入力が終わったら［*OK*］をクリックして確定します。

キーボードタブ

「キーボード」タブを使用して、キーボードのレイアウトやグラフィカルコンソールの指定ができます。

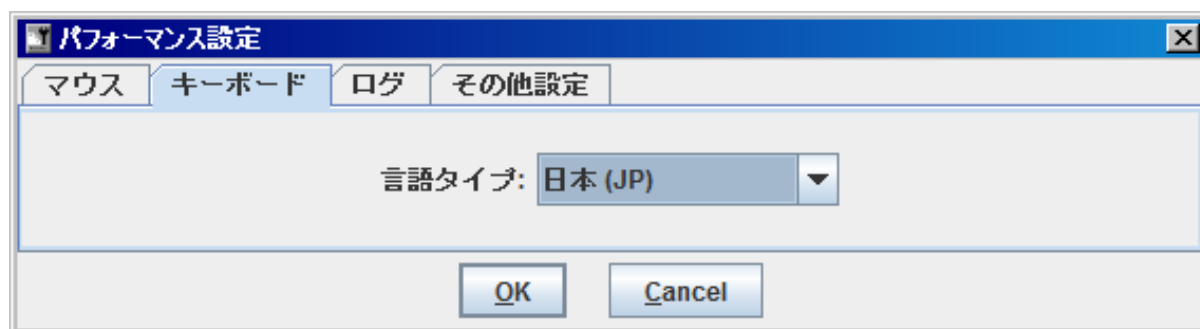



図 66 : 「パフォーマンス設定」メニュー - 「キーボード」タブ

言語

グラフィカルコンソールのキーボードレイアウトを選択します。

i 管理対象サーバのキーボードレイアウトも同様に設定する必要があります。

➤ 入力が終わったら［*OK*］をクリックして確定します。

ログ作成タブ

「ログ」タブはログ作成設定の設定に使用します。

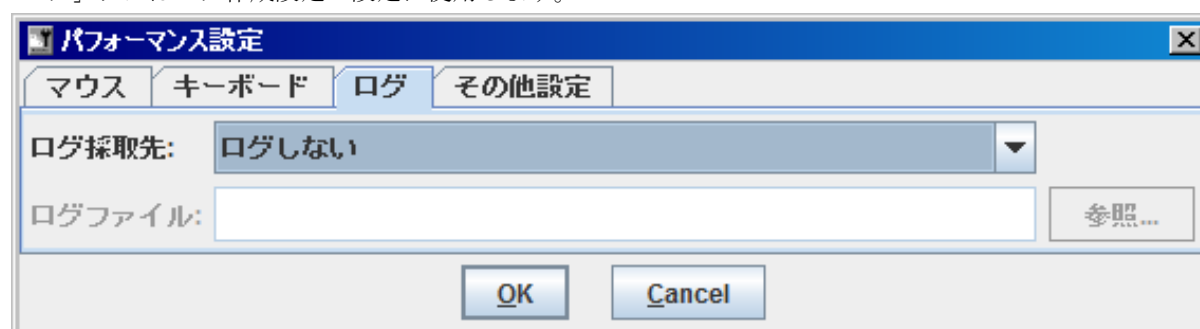



図 67 : 「パフォーマンス設定」メニュー － 「ログ」タブ

i 「ログしない」に設定しなければなりません！

➤ 入力が終わったら［*OK*］をクリックして確定します。

その他設定タブ

「その他設定」タブは、iRMC S2 で AVR セッションのハードウェア圧縮を行うかどうかを設定します。

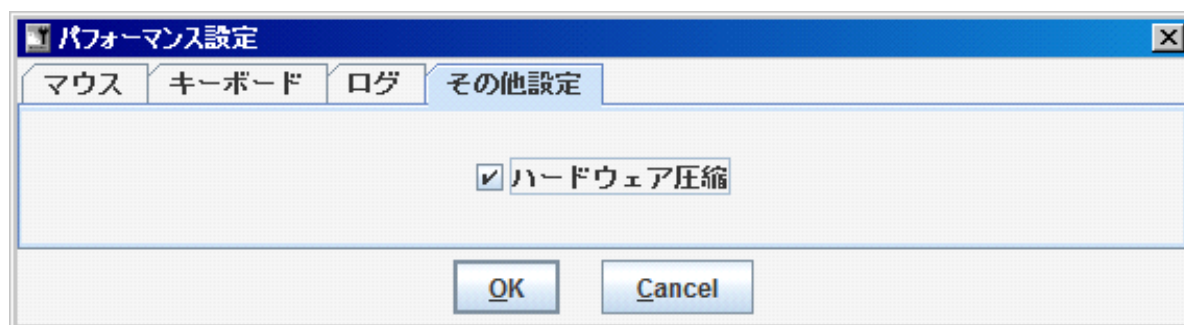



図 68：「パフォーマンス設定」メニュー –「その他設定」タブ

ハードウェア圧縮

このオプションを有効にすると、iRMC S2 は AVR セッションのハードウェア圧縮を実行します。

➤ 入力が終わったら［*OK*］をクリックして確定します。

6 章 リモートストレージ

リモートストレージ機能を使用するには有効なライセンスキーが必要です。

リモートストレージはネットワーク上にどこにでも置ける「バーチャル」ドライブを使用可能とします。2 個のメディアまでリダイレクトすることができます。

バーチャルドライブのソースは次のように選ぶことができます。

- AVR Java アプレットを使用するリモート管理端末の物理ドライブまたはイメージファイルをとして。（180 ページを参照してください。）
- リモートストレージサーバ経由ネットワークセントラルの CD/DVD ISO イメージとして。（194 ページを参照してください。）

パラレルリモートストレージ接続

以下は同時実行することが可能です。

- 最大 2 台のリモート管理端末のバーチャルドライブへのリモートストレージ接続（接続が AVR Java アプレット上で確立されている場合）

  または

- 1 台のリモートストレージサーバへのリモートストレージ接続。

アプレット経由とリモートストレージサーバ経由のリモートストレージ接続を同時に確立させることはできません。

iRMC S2 Web インターフェースの「*Remote Storage*」ページを使用して、現在のリモートストレージ接続のステータス情報を取得し、リモートストレージサーバへの接続を確立することができます。（353 ページを参照してください。）

6.1 リモート管理端末上のリモートストレージの規定

リモート管理端末上のバーチャルドライブのソースを規定すれば、リモートストレージ機能は以下のデバイスタイプをサポートします。

- Floppy
- CD ISO イメージ
- DVD ISO イメージ

バーチャルドライブはリモート管理端末から PRIMERGY サーバにオペレーティングシステムをインストールする場合にも使用可能です。(451 ページ、「iRMC S2 によるオペレーティングシステムのリ モートインストール」の章を参照してください。)

本節では次の点について説明します。

- リモートストレージの起動
- リモートストレージのストレージメディアの規定
- ストレージメディアのリモートストレージへの接続
- リモートストレージ接続の解除
- リモートストレージに使用可能としたメディアの取り出し

6.1.1 リモートストレージの開始

リモートストレージ機能は、AVR Java アプレットを使用して開始します。(344 ページ、「ビデオリ ダイレクションービデオリダイレクション (AVR) の開始」の節を参照してください。)

➢ iRMC S2 Web インターフェースを起動します（210 ページの「iRMC S2 の Web インターフェー スへのログイン」を参照してください。)

➢「Advanced Video Redirection」ページを開いて [Start Video Redirection] ボタンをクリックし、ビデオリダイレクションを起動させます。(344 ページ、「ビデオリダイレクションービデオリダ イレクション (AVR) の開始」の節を参照してください。)

その結果 AVR ウィンドウが開かれます。

➢ AVR ウィンドウのメニューバーから、以下を選びます。

Remote Storage - Remote Storage...

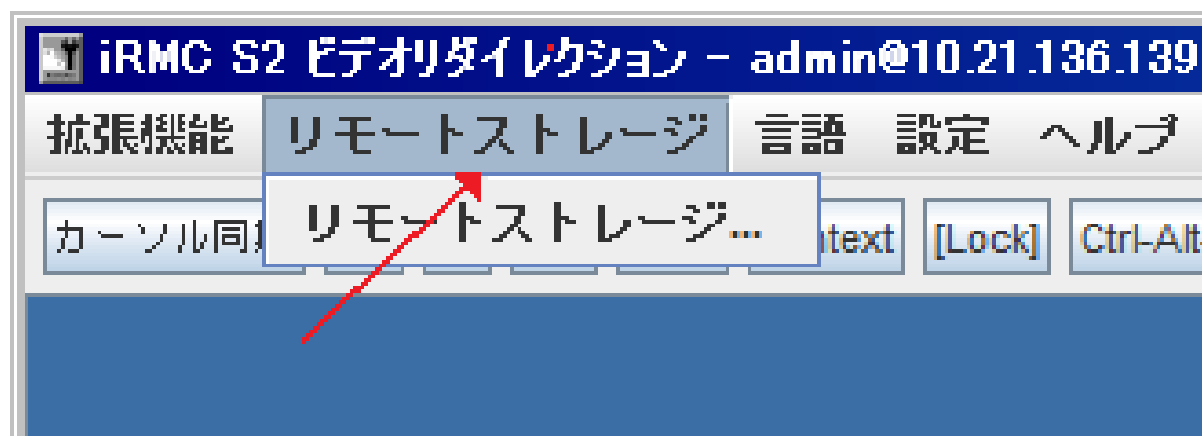



図 69:「iRMC S2 ビデオリダイレクション」ウィンドウ –「リモートストレージ」-「リモー トストレージ」

「ストレージデバイス」ダイアログボックスが開き、現在リモートストレージとして使用可能なストレージメディアがリストされます。

Windows システムの「ストレージデバイス」ダイアログボックス

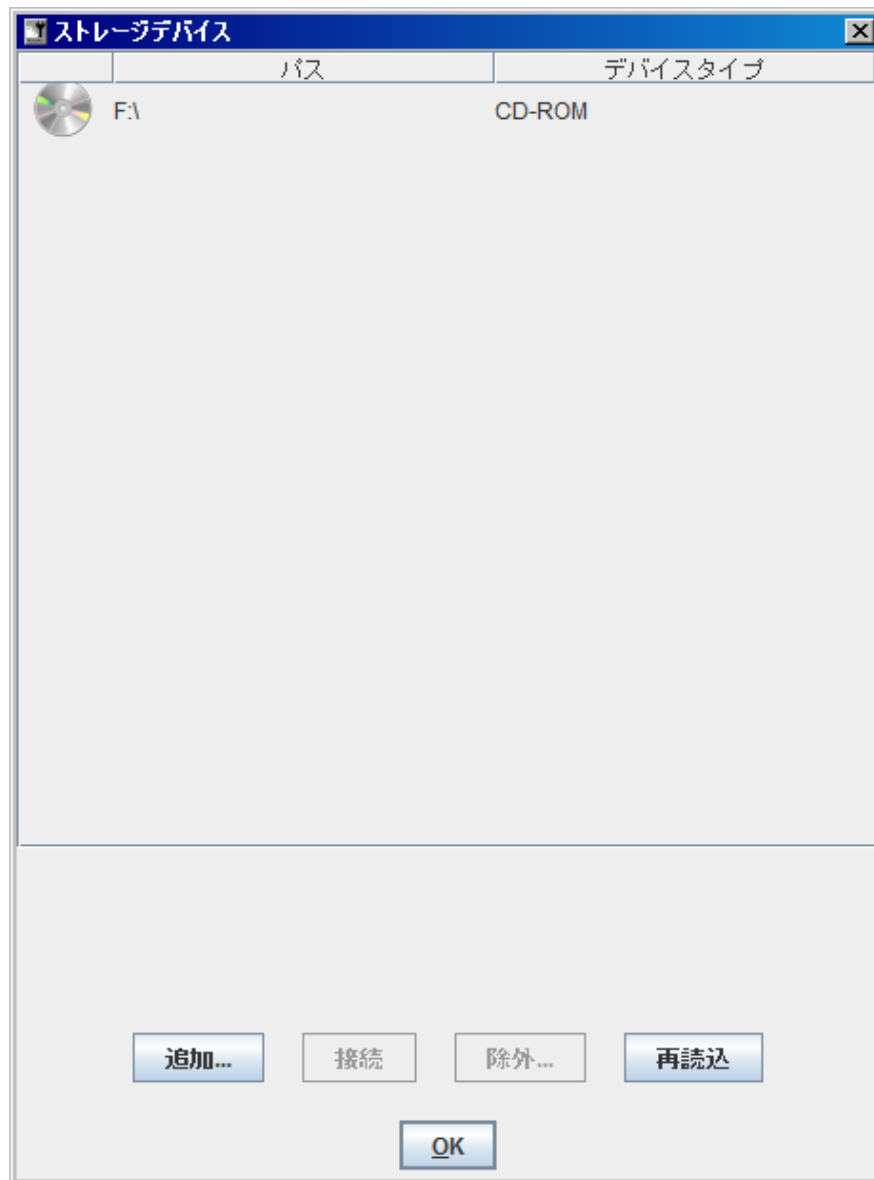



図 70 :「ストレージデバイス」ダイアログボックス

光学ドライブ（CD ROM、DVD ROM）にストレージメディアが挿入されていれば、コンテンツは自動的に表示されます。
ストレージメディアが挿入されていてもコンテンツが自動的に表示されない場合には、ストレージメディアはローカルのエクスプローラに占有されています。

Linux システムの「ストレージデバイス」ダイアログボックス

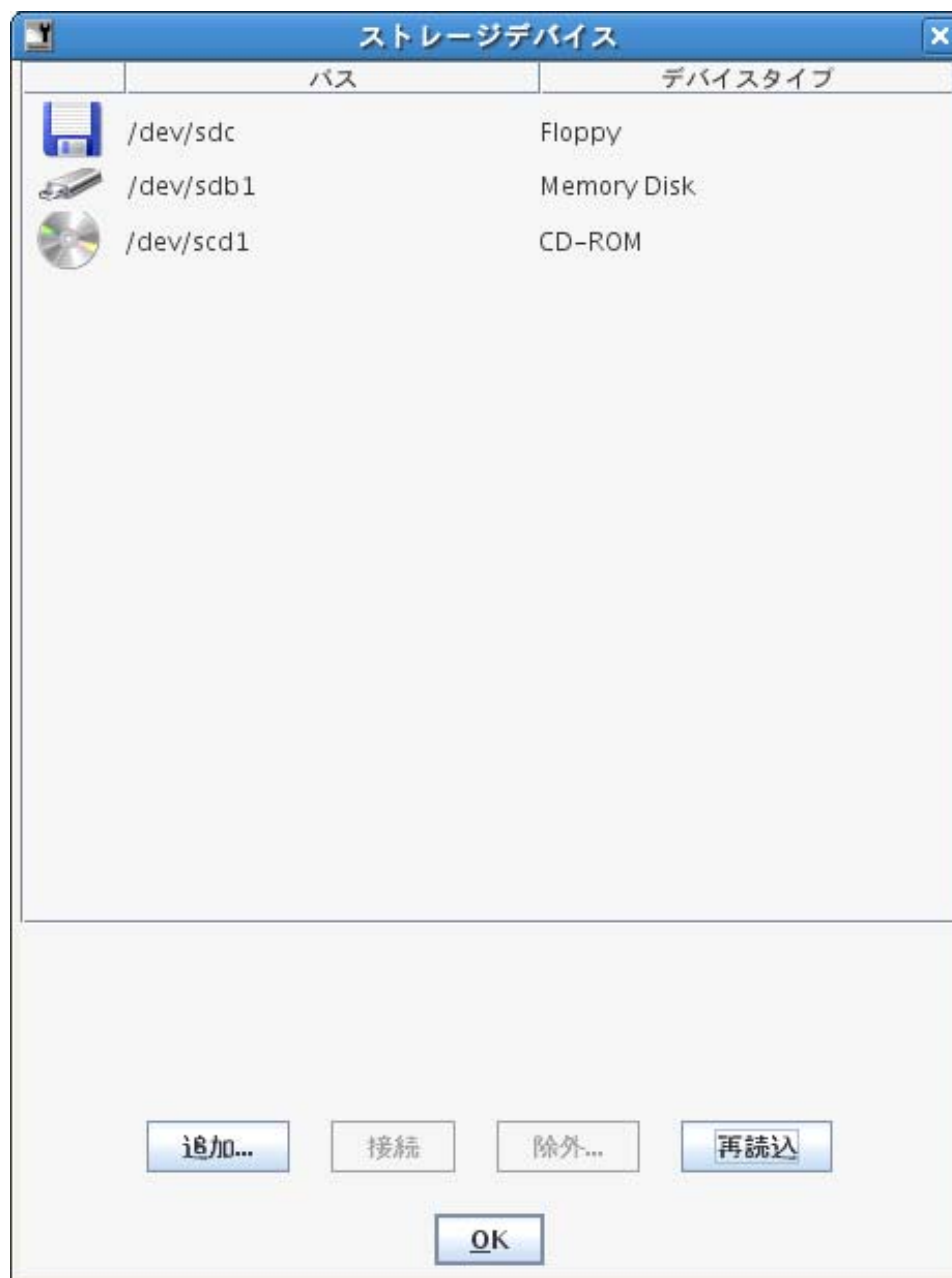



図 71 :「ストレージデバイス」ダイアログボックス

物理ストレージメディアがマウントされリモートストレージデバイスとして接続できなければなりません。マウントされたストレージメディアは「ストレージデバイス」ダイアログボックスに自動的に表示されます。

6.1.2 リモートストレージのストレージメディアの追加

➢ *「ストレージデバイス」ダイアログボックスで［追加］をクリックします。「ストレージデバイスの追加」ダイアログボックスが開きます。*

Windows システムの「ストレージデバイスの追加」ダイアログボックス

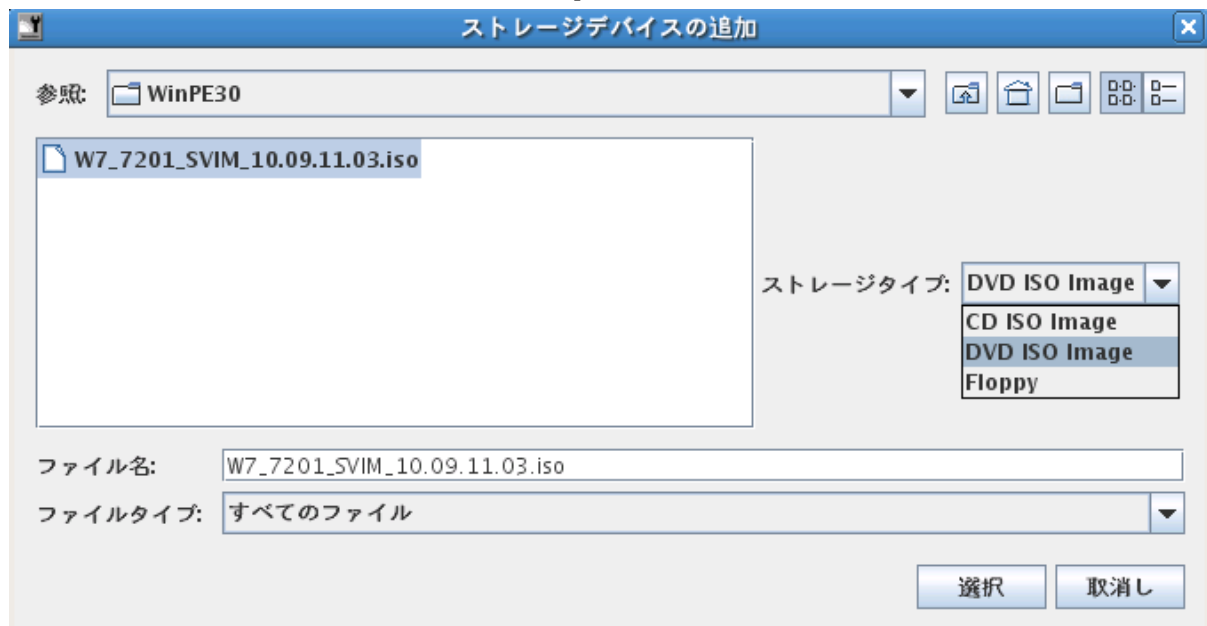



図 72 :「ストレージデバイスの追加」ダイアログボックス (Windows)

Linux システムの「ストレージデバイスの追加」ダイアログボックス

図 73 :「ストレージデバイスの追加」ダイアログボックス (Linux)

- 「ストレージデバイスの追加」ダイアログボックスで、現在のリモート管理端末からリモートストレージとして使用可能にしたいリモートストレージメディアのディレクトリに移行します。
- 「ストレージタイプ」の下から必要なデバイスのタイプを選択します。

以下のタイプのストレージを選択できます。

- Floppy
- CD ISO イメージ
- DVD ISO イメージ

i 物理ストレージデバイスを Linux システムにマウントする必要があります。

- リモートストレージとして接続したいストレージメディアを「ファイル名」の下に指定します：
  - ISO image (ISO/NRG image) である場合には、ファイル名を入力してください。

    または、エクスプローラでファイル名をクリックしてください。
  - ドライブである場合には、ドライブ名を入力してください。たとえば、
    - ドライブ D の「D」(Windows)
    - /dev/... (Linux)

「ストレージデバイスの追加」ダイアログボックス： ストレージメディアの選択（*Windows)*

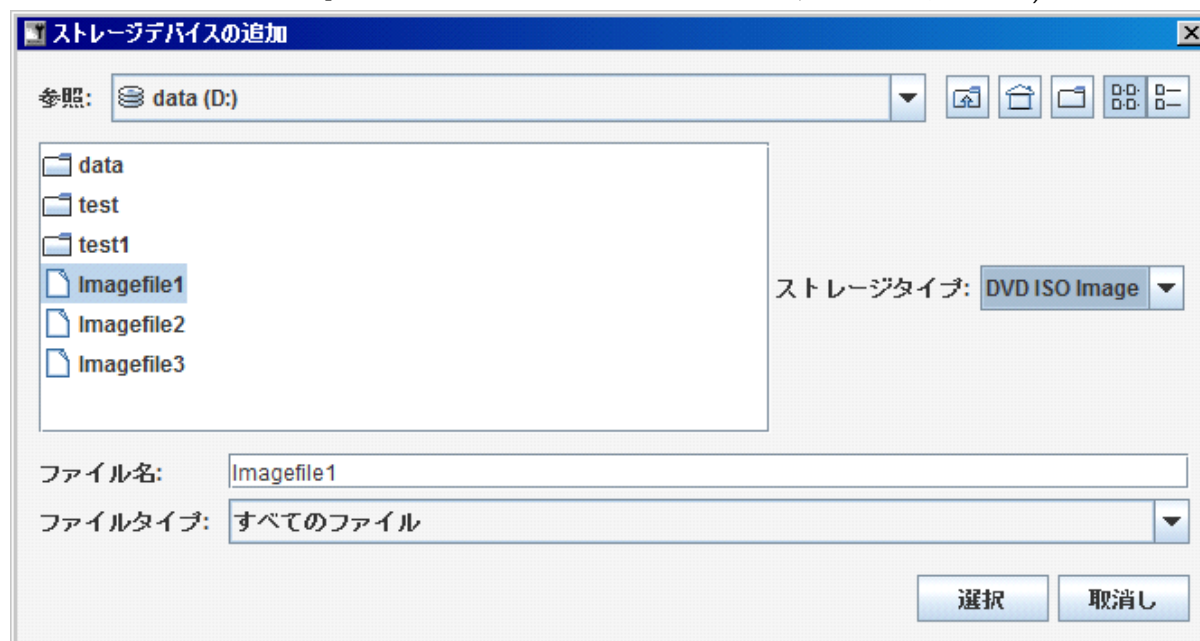



図 74 :「ストレージデバイスの追加」ダイアログボックス：ストレージメディアの選択

［ストレージデバイスの追加］ダイアログ： ストレージメディアの選択 (Linux)

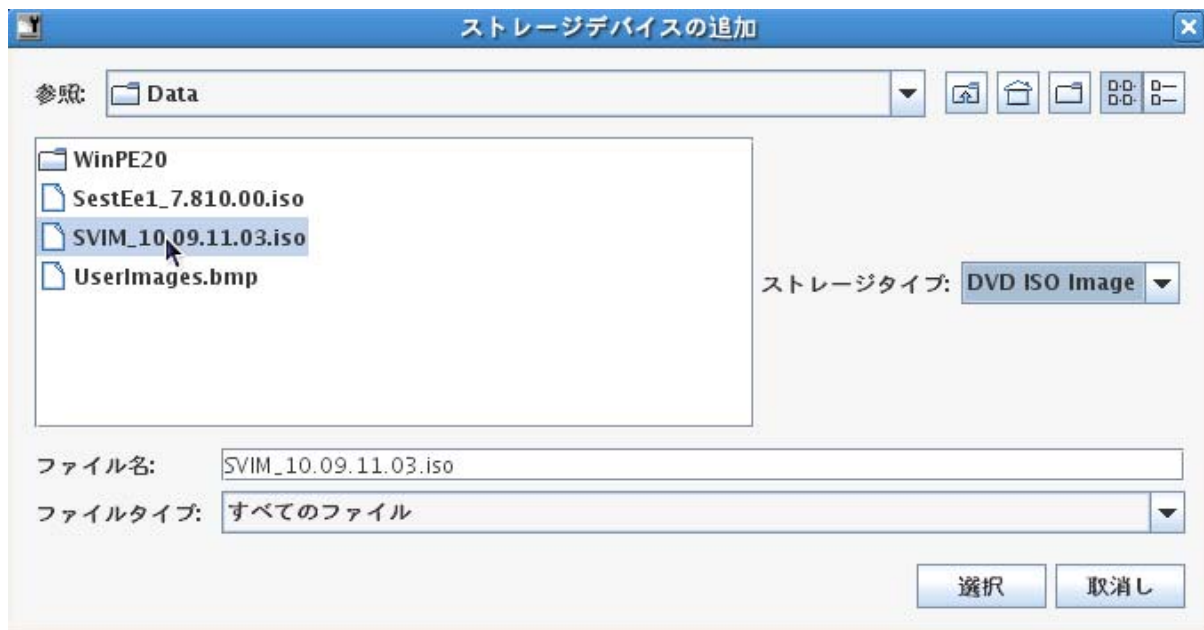



図 75： 「ストレージデバイスの追加」ダイアログボックス： ストレージメディアの選択

➤ ［選択］クリックして選択を確定します。

選択されたストレージメディアがリモートストレージとして使用可能になり、「ストレージデバイス」ダイアログボックスに表示されます。

「ストレージデバイス」ダイアログボックスの表示 (*Windows)*

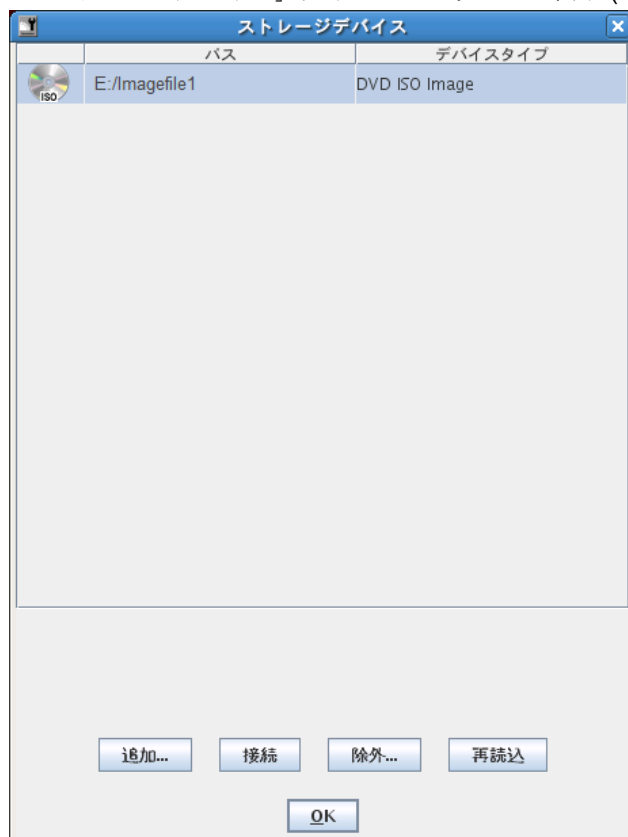



図 76： ストレージデバイスダイアログボックス： 追加されたストレージメディアが表示される

「ストレージデバイス」ダイアログボックスの表示 (*Linux*)

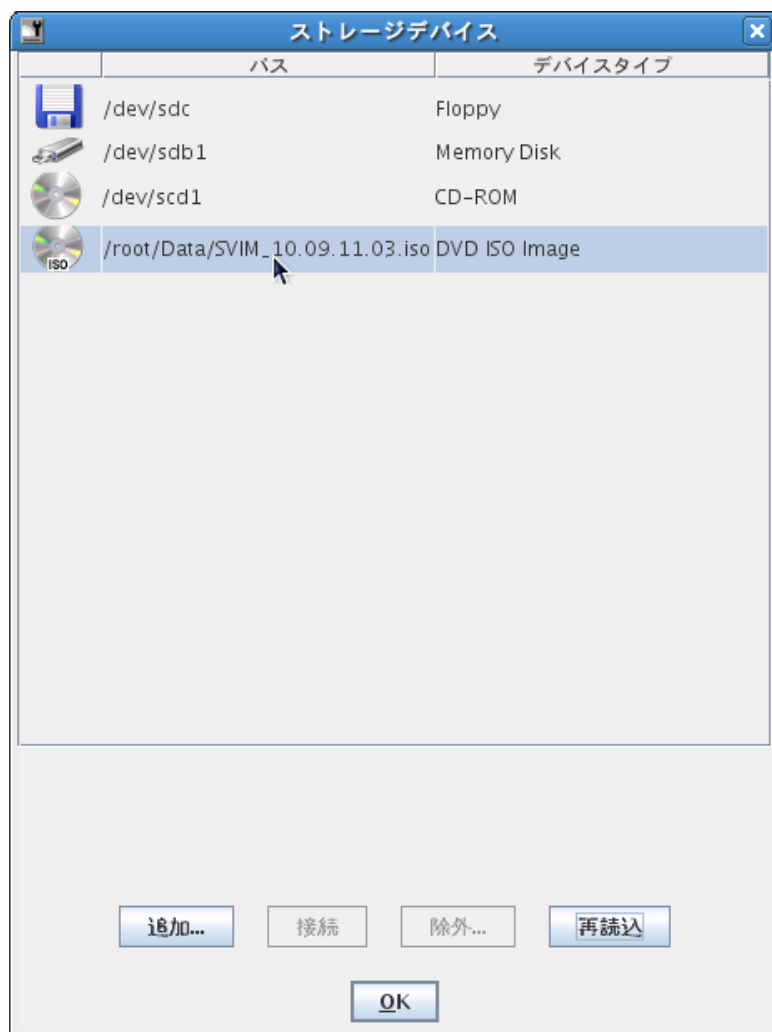



図 77 :「ストレージデバイス」ダイアログボックス： 追加されたストレージメディアが表示される

6.1.3 ストレージメディアのリモートストレージの接続

- ➤「ストレージデバイス」ダイアログボックス（図 76 および 図 77 参照）で、リモートストレージとして接続したいストレージメディアをクリックします。
- ➤［接続］をクリックして、選択したストレージメディアをリモートストレージとして接続してください。

「ストレージデバイス」ダイアログボックスが開き、安全な取り外しに関するメッセージが表示されます。ストレージメディアがリモートストレージとして接続されます。

> i 2 台のストレージデバイスをリモートストレージとして同時に接続したい場合は、接続が確立される前に確認ダイアログボックスが表示されます。(191 ページ、「2 台のスト レージデバイスのリモートストレージとしての同時接続」を参照してください)

ストレージデバイスダイアログボックス： リモートストレージ接続の表示 (Windows)

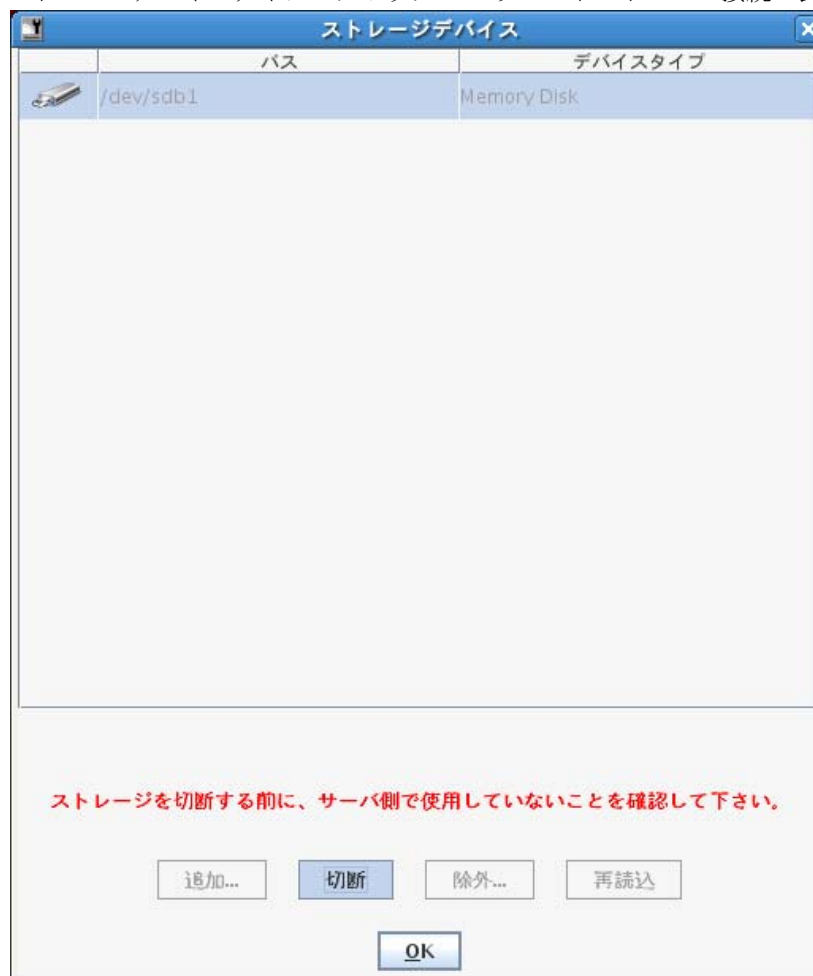



図 78 :「ストレージデバイス」ダイアログボックス：ストレージメディアがリモートストレージ として接続される。

ストレージデバイスダイアログボックス： リモートストレージ接続の表示 (Linux)

図 79 :「ストレージデバイス」ダイアログボックス：ストレージメディアがリモートストレージとして接続される。

ストレージデバイスダイアログボックス： リモートストレージ接続の表示 (Linux)

図 79 :「ストレージデバイス」ダイアログボックス：ストレージメディアがリモートストレージとして接続される。

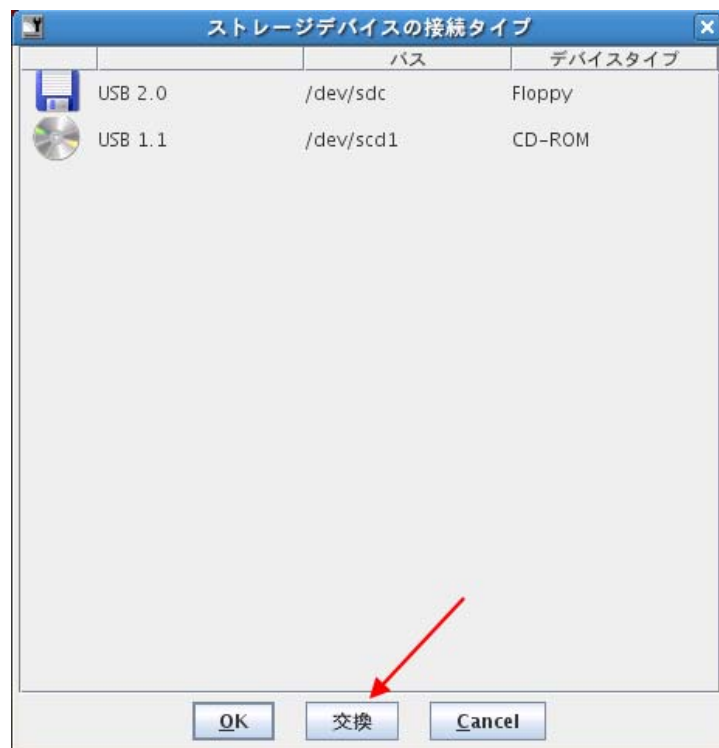



図 81： 「ストレージデバイスの接続タイプ」ダイアログボックス： USB 1.1 および USB 2.0 の割り当て

➤ ストレージデバイスの USB 1.1 と USB 2.0 への割り当てを入れ替えたい場合には［交換］をクリックしてください。

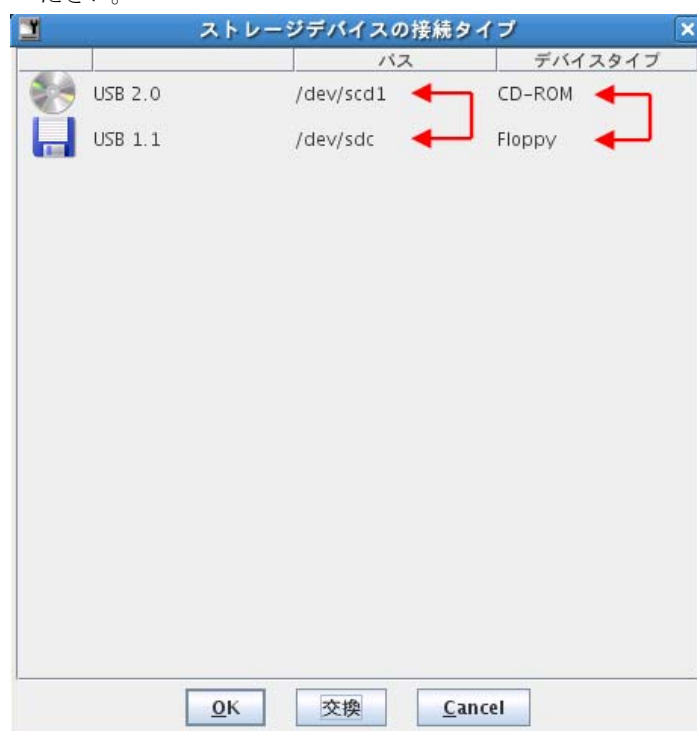



図 82 :「 ストレージデバイスの接続タイプ」ダイアログボックス： 入れ替えられた USB 1.1 と USB 2.0 の割り当て

➤ ［*OK*］をクリックして、ストレージデバイスをリモートストレージとして接続してください。

6.1.4 リモートストレージ接続の切断

➢「ストレージデバイス」ダイアログボックスを開いてください。(182 ページ、「リモートストレージの開始」の節を参照してください。)

リモートストレージとして接続されたストレージメディアのリストが表示されます（Windows の例です）。

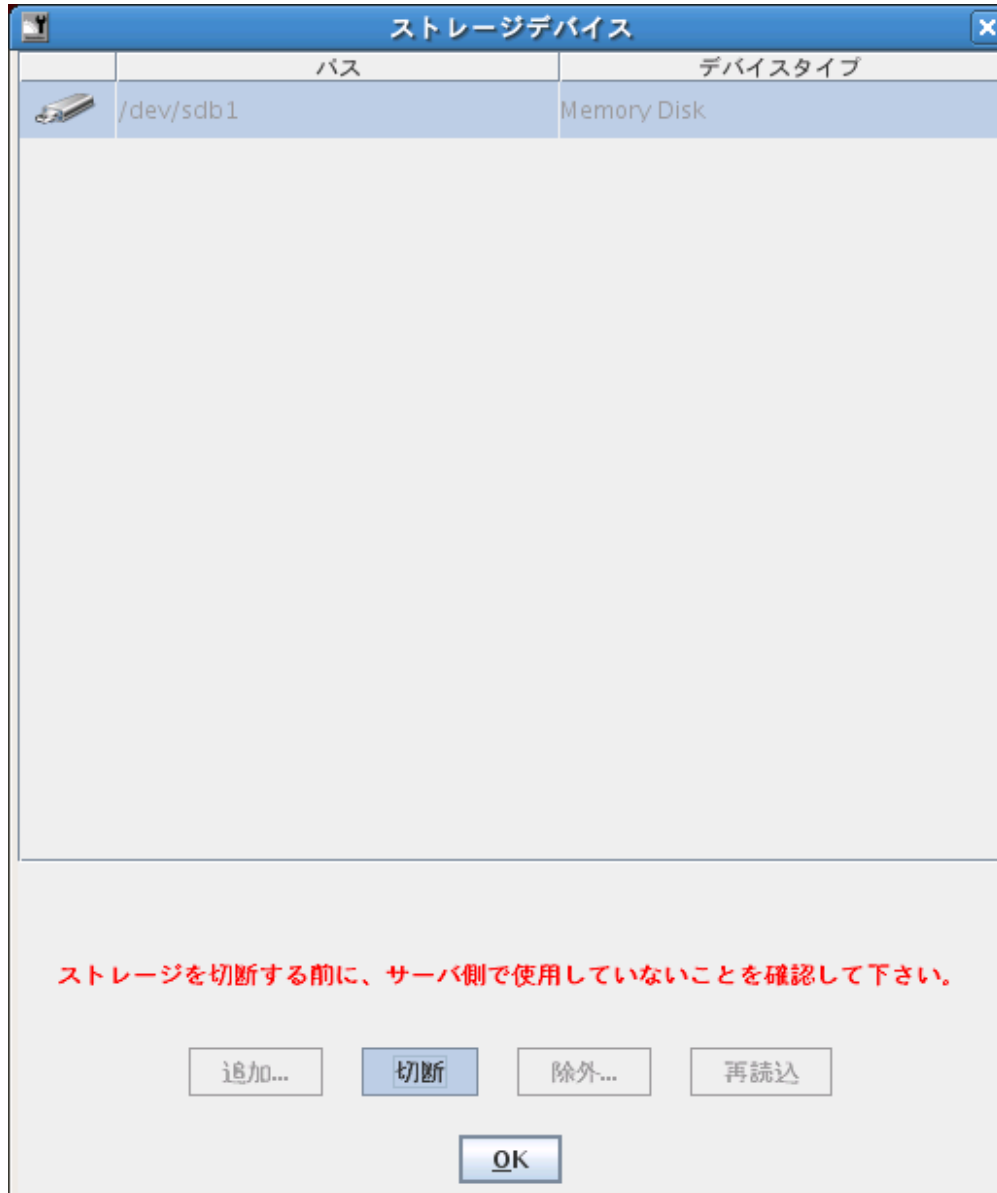



図 83： 「ストレージデバイス」ダイアログボックス： リモートストレージの切断

➢「安全な取り外し」、すなわちストレージメディアにアクセスしているアプリケーションやプログラムがないことを確認してください。

➢［切断］をクリックして、すべてのリモートストレージ接続を解除してください。

6.1.5 ストレージメディアの除外

以下の通りストレージメディアをリモートストレージに使用可能なメディアのリストから除外してください。

➤ 「ストレージデバイス」ダイアログボックスを開いてください。（182 ページ、「リモートストレ ージの開始」の節を参照してください。）

リモートストレージとして使用可能なストレージメディアのリストが表示されます（Windows の例です

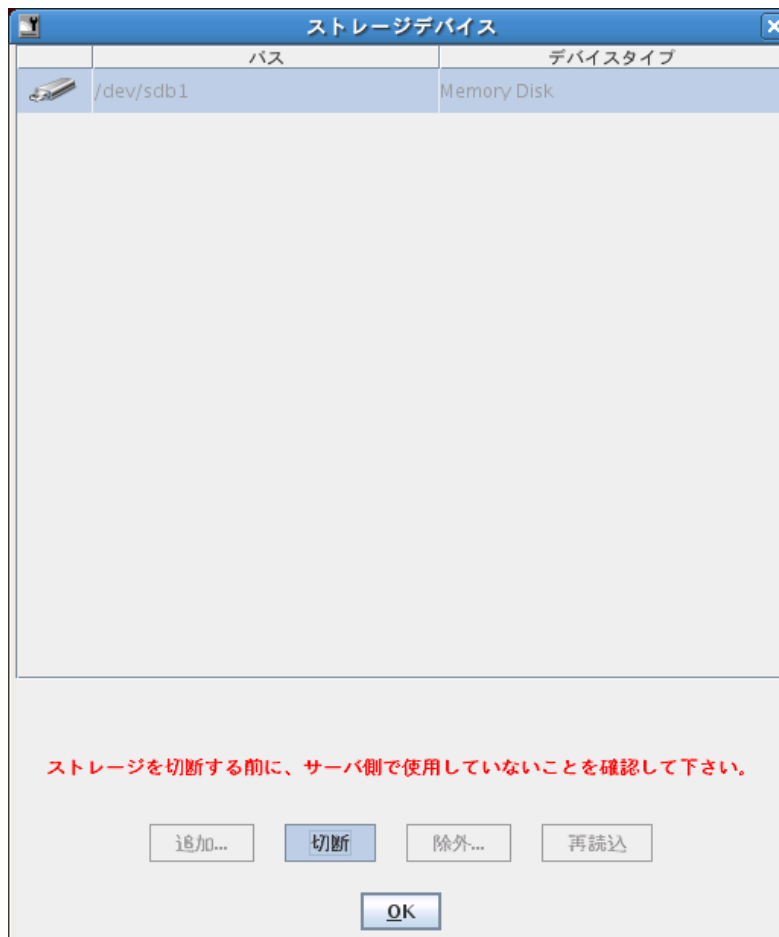



図 84 :「ストレージデバイス」ダイアログボックス：リモートストレージメディアの除外

➤ 取り出したいストレージメディアを選択してください。

➤ ［除外…］をクリックしてストレージメディアを除外してください

6.2 リモートストレージサーバを経由するリモートストレージの追加

リモートストレージサーバを利用して、iRMC S2 によって管理され、PRIMERGY サーバが何台でもリモートストレージとして使用できるイメージファイル（ISO/NRG イメージ）を追加することができます。このイメージファイルを使用してリモート管理端末から 1 台または複数の PRIMERGY サー バをブートすることができます。（451 ページ、「iRMC S2 によるオペレーティングシステムのリモー トインストール」の章を参照してください。）

リモートストレージサーバは Windows システムにも Linux システムにも使用することができます。リモートストレージサーバは Windows と Linux の両方で、32 ビットと 64 ビットのどちらのバリアントでも使用可能です。

リモートストレージサーバの個々のバリアントは ServerView Suite の DVD 1 の中で、「*SVSoftware¥Software¥RemoteView¥iRMC*」の下にあります。

PRIMERGY サーバがリモートストレージ経由で使用可能な ISO イメージの作成

お使いの PRIMERGY サーバで、リモートストレージサーバにより使用可能にされたイメージファイルを使用する場合は、以下の要件を満たさなければなりません。

- リモートストレージサーバがインストールされていること (196 ページと 207 ページを参照してください。)
- リモートストレージサーバが起動されていること（206 ページと 208 ページを参照してください。）
- 管理対象サーバの iRMC S2 がリモートストレージサーバに接続されていること（353 ページを参照してください。）

WinPE 2.x– ベースの **ISO** イメージからのブート

iRMC S2 が稼働し 3.60A 以前のファームウェアの場合は、PRIMERGY サーバは WinPE 2.**x**– ベースの ISO イメージからのブートする必要があります。（たとえば、Windows サーバ 2008 および ServerView Installation Manager。）

6.2.1 Windows の下のリモートストレージサーバ

リモートストレージサーバは 32 ビット版でも 64 ビット版でも使用できます。64 ビットシステムに、同時に 32 ビット版と 64 ビット版のリモートストレージサーバを同時にインストールすることはできません。

6.2.1.1 リモートストレージサーバのインストール

リモートストレージサーバのインストール用の「*RemoteStorageServer_Installer32.exe*」と

「*RemoteStorageServer_Installer64.exe*」インストールプログラムはそれぞれ ServerView Suite の DVD 1 の中の

「*SVSoftware¥Software¥RemoteView¥iRMC¥Widows_32*」と
「*SVSoftware¥Software¥RemoteView¥iRMC\Widows_x64*」の下にあります

以下の説明は、32 ビットバリアントのインストールに関するものです。64 ビットバリアントも同じ方法で進めてください。

➢「*RemoteStorageServer_Installer32.exe*」を起動してリモートストレージサーバをインストールします。

インストールプログラムの「ようこそ」の画面が現れます：

図 85： リモートストレージサーバのインストール 「Welcome」画面

➢ ［*Next*］ボタンをクリックしてください。

指定されたインストール用ディレクトリが表示されます。(図 86 を参照してください。

図 86： リモートストレージサーバのインストール：インストール用フォルダの指定

- リモートストレージサーバをデフォルトのフォルダ以外にインストールする場合は、［*Browse...*］をクリックして使用したいディレクトリに移動してください。

- ［*Next*］ボタンをクリックしてください。

  スタートメニューにプログラムショートカットが表示される場所を選択するためのこのウィンドウが立ち上がります。(図 87 を参照してください。

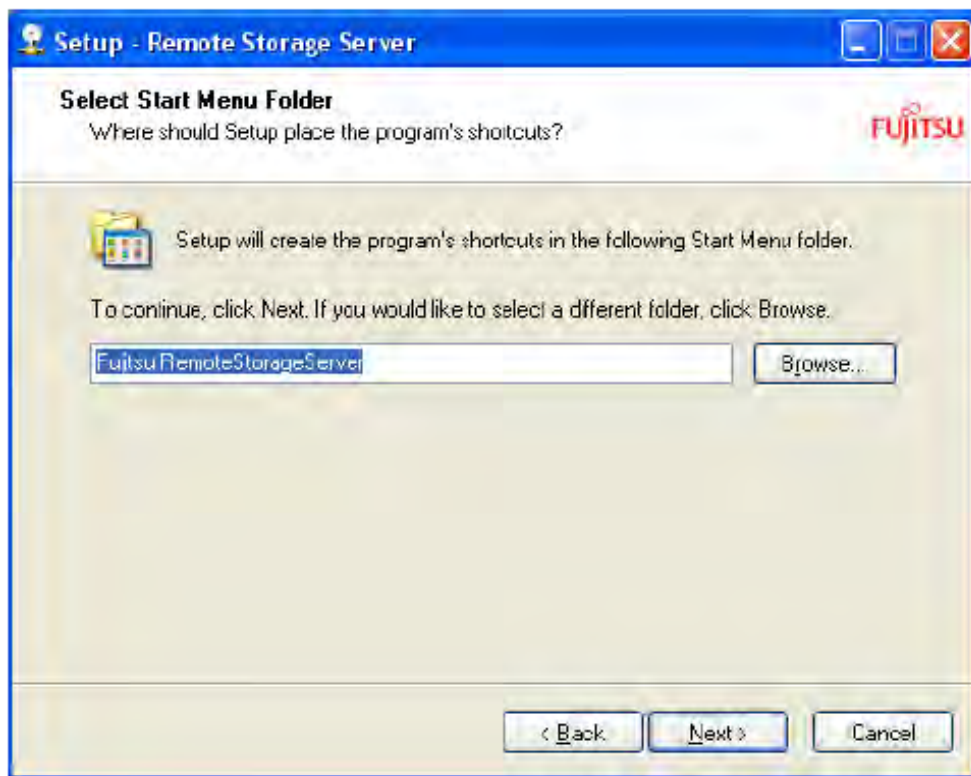



図 87 : リモートストレージサーバのインストール：インストール用フォルダの指定

➤ プログラムショートカットをデフォルトのフォルダ以外のフォルダに置きたい場合は、［*Browse...*］をクリックして使用したいフォルダを指定します。

➤［*Next* ］ボタンをクリックしてください。

「*Ready to Install*」ウィンドウが開きます。ここで、これまで行った設定を確認した後、リモートストレージサーバのインストールを開始します。（図 88 を参照してください。）

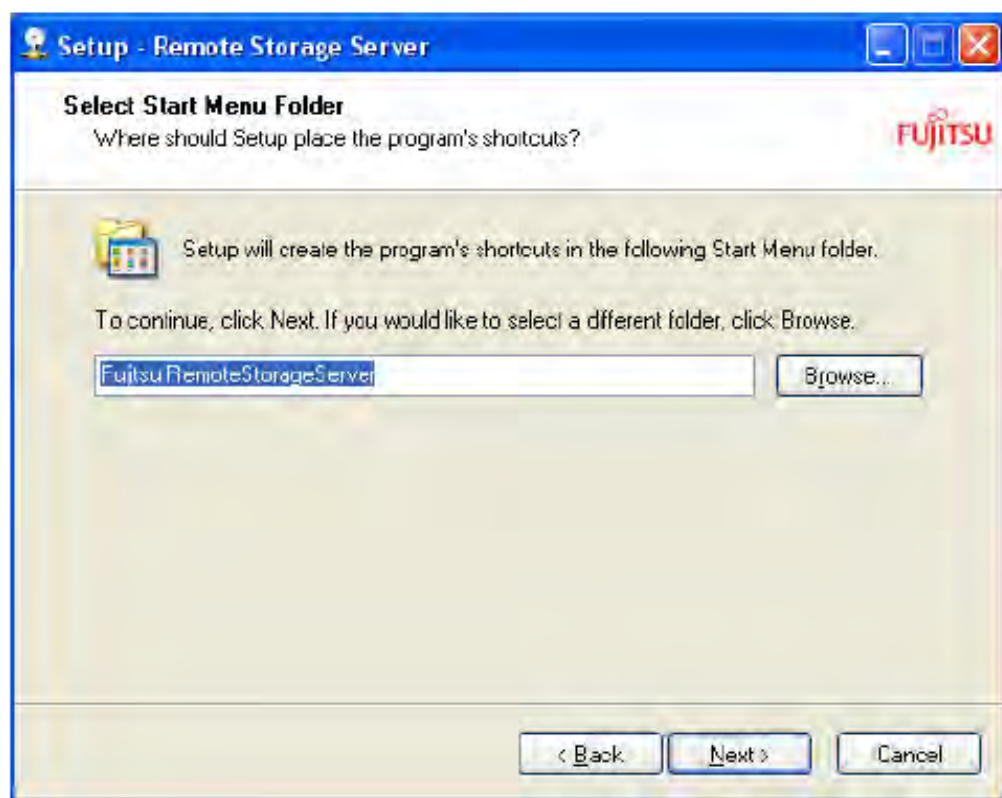



図 88： リモートストレージサーバのインストール：インストールの開始

➢［*Install*］をクリックしてリモートストレージサーバのインストールを開始させます。
インストールが完了すると 図 89 に示されたウィンドウが表示されます。

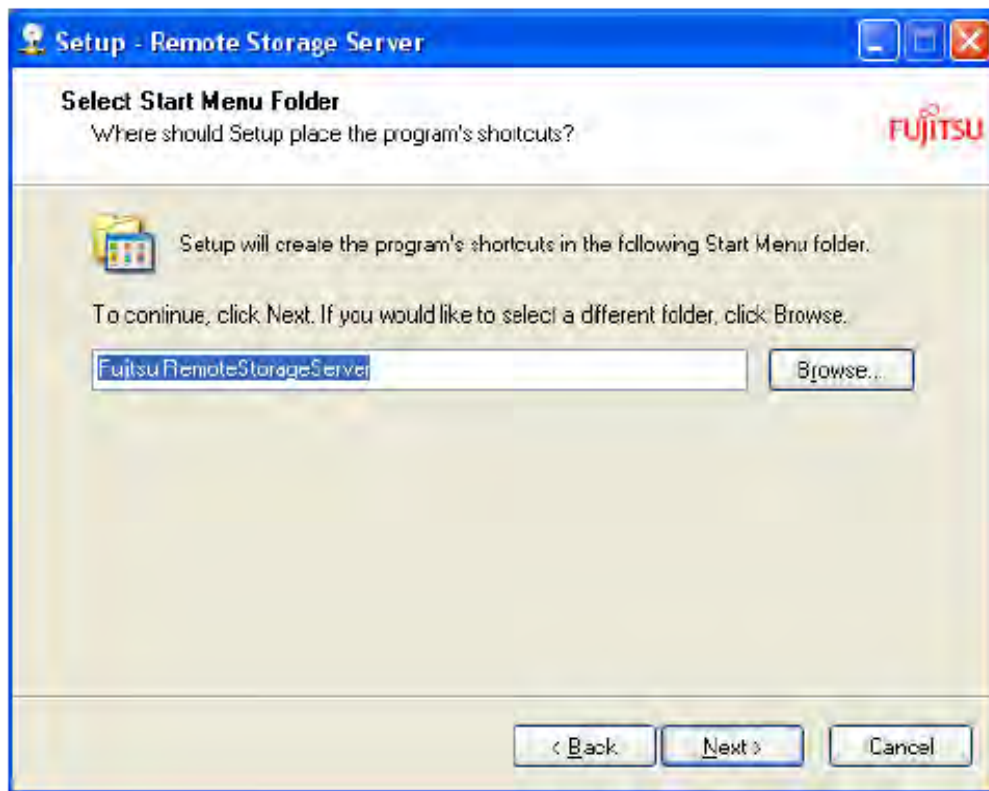



図 89： リモートストレージサーバのインストール：インストールプログラムを閉じる

「*Launch Remote Storage Server*」オプションが確認され、インストール用プログラムが閉じられると、リモートストレージサーバの GUI （203 ページ参照）が起動します。

➤［*Finish*］をクリックして、インストールプログラムを閉じてください。

6.2.1.2 リモートストレージサーバの実行モード

リモートストレージサーバは必要に応じて以下のモードで実行することができます。

- バックグラウンドのサービスとして
- スタンドアローンプログラムとして

リモートストレージサーバの実行モードはグラフィカルユーザーインターフェースを使って設定します。(203 ページを参照してください。)

リモートストレージサーバのサービスとしての実行

以下の点に注意が必要です。

- イメージファイルは、ネットワーク上のコンピュータにも、リモートストレージサーバが稼働しているのと同じホストにも、どちらにも置くことができます。

> i イメージファイルをリモートストレージサーバが稼働しているのコンピュータ以外に置く場合には、イメージファイルのパスを UNC 表記で指定しなければなりません。また、イメージファイルのアクセス権限があるユーザーカウントも必要です。

- リモートストレージサーバが置かれたホストをブートすると、リモートストレージサーバも自動的にブートします。リモートストレージサーバはその後、明白に終了させられるかホストがシャットダウンされるまで実行されます。
- リモートストレージサーバが置かれたホストをブートすると、イメージファイルは自動的に使用可能になります。

6.2.1.3 リモートストレージサーバの設定、起動、および、終了

リモートストレージサーバはグラフィカルユーザーインターフェース (GUI) を使用して設定、起動および終了します。

リモートストレージサーバのグラフィカルユーザーインターフェース呼び出し

リモートストレージサーバのグラフィカルユーザーインターフェースを以下の通り呼び出してください。

Ø次のように選択します :「*Start*」→「*Programs*」→「*Fujitsu RemoteStorageServer*」→「*Remote Storage Server*」。

リモートストレージサーバのグラフィカルユーザーインターフェースが表示されます。

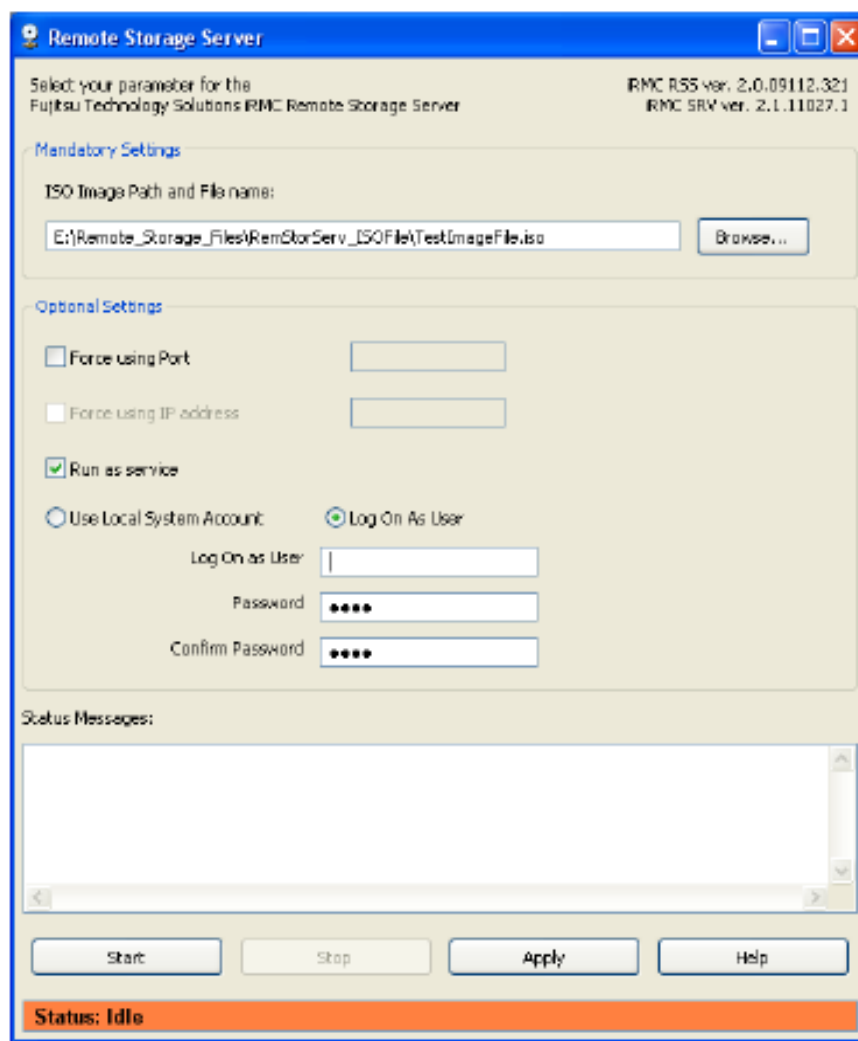



図 90 : リモートストレージサーバのグラフィカルユーザーインターフェース（この例では「アイドル」状態）

リモートストレージサーバの設定

i　設定は、リモートストレージサーバが「アイドル」状態にあるとき、すなわち実行されていないときのみ可能です。

グラフィカルユーザーインターフェースで、リモートストレージとして実行可能にするイメージファイルを他のパラメータと合わせて指定してください。

ISO イメージのパスとファイル名：

Øイメージファイルのパスと名前をフィールドに直接入力してください。または

Ø［*Browse...*］ボタンをクリックし、次に、「Choose a file」ダイアログに移動して必要なイメージファイルを選択し、確定します。

i　リモートストレージサーバをサービスとして稼働させる場合（205 ページ「Run as Service」オプション参照）および、イメージファイルをネットワーク上のコンピュータに置く場合は、イメージファイルのパスを UNC 表記で指定する必要があります。また、「Log On As User」（205 ページ 参照）の下に入力したアカウントが有効であり、イメージファイルが置かれた領域を共有するアクセス権限があることを確認しなければなりません。

ポート番号による指定

iRMC S2 のリモートストレージポートに初期値のポート番号 (5901) 以外のポート番号を設定した場合（296 ページまたは 409 ページ参照）、このオプションを有効化し、設定したポート番号を関連するフィールドに入力する必要があります。

IP アドレスによる指定

リモートストレージサーバが実行されるホストが複数の LAN 接続されている場合は、リモートストレージサーバがサービスとして実行される場合には、それに使用される LAN 接続に IP アドレスを指定することができます。

初期設定では、リモートストレージサーバは最初に検出された LAN 接続を使用します。

サービスとしての稼働

リモートストレージサーバがバックグラウンドでサービスとして実行される場合にはこのオプションを有効にして下さい。(202 ページを参照してください。)

Ø次の 2 つのオプションからどちらかを選択します。

ローカルのシステムアカウント使用

リモートストレージサーバはローカルのシステムアカウントに下でサービスとして実行されます。

この場合には、イメージファイル（ISO/NRG イメージ）をローカルのドライブに置くことはできません。

ユーザーとしてログオン

リモートストレージサーバは下記の入力フィールドに指定されたユーザーカウントで実行されます。

ユーザー名を以下の書式で指定してください。

- ローカルユーザーには、. ¥Logon-Name
- ドメインユーザーには、

  DOMAIN\LogOnName

  または

  LogOnName@DOMAIN<mailto:LogOnName@DOMAIN>

イメージファイルは、「*Log On As User* 」オプションが有効になっていれば、ネットワークドライブに置くことができます。この場合は、指定されたアカウントにはイメージファイルが置かれたネットワークドライブのアクセス 権限が必要です。また、イメージファイルは UNC 表記で指定しなければなりません。(204 ページの入力フィールド「ISO Image Path or Filename」を参照してください。)

➤［*Apply* ］ボタンをクリックして設定を有効にしてください。

リモートストレージサーバの開始

➤［*Start*］ボタンをクリックしてリモートストレージサーバをサービスとして、または、スタンドアローンとして開始させます。

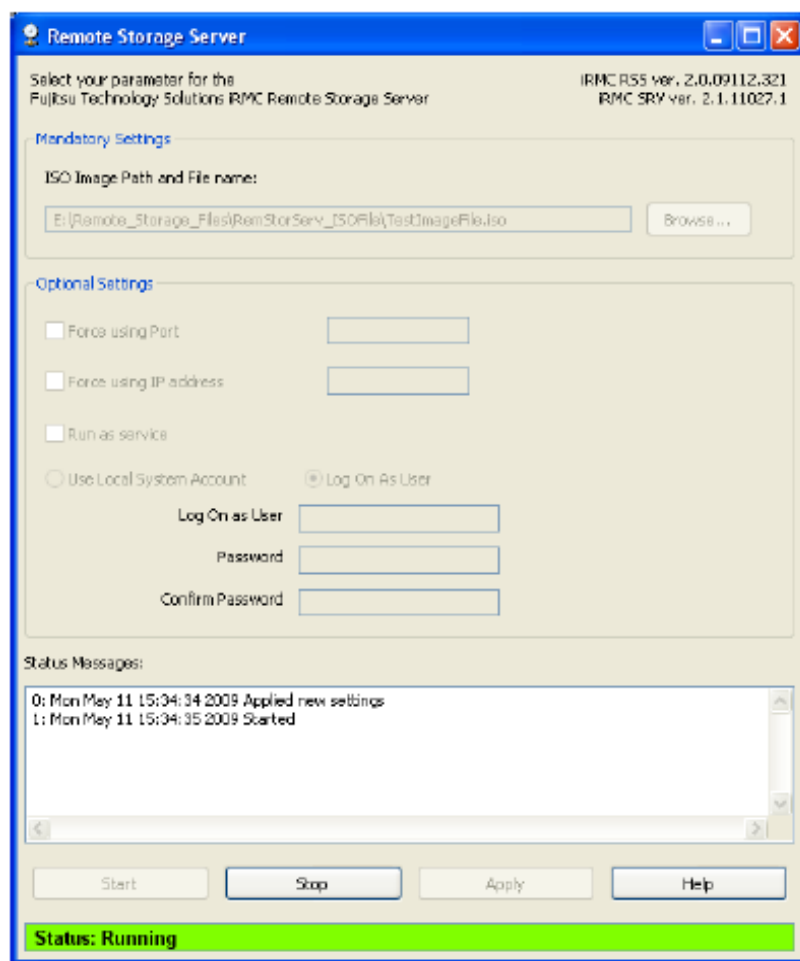



図 **91**： リモートストレージサーバが実行されました（「稼働」状態）

ステータスメッセージ
　作成されたリモートストレージサーバの実行ステートのログがここに表示されます。

i　実行モードが「*Run as service*」に設定されている場合は（205 ページ参照）、リモートストレージサーバはリモートストレージサーバがインストールされたコンピュータが ブートされたときに自動的に起動されます。

i　リモートストレージサーバの実行は、グラフィカルユーザーインターフェースを終了させても自動的に中断されることはありません。

リモートストレージサーバの終了

➤［*Stop* ］ボタンをクリックしてリモートストレージサーバの実行を終了させます。

6.2.2 Linux によるリモートストレージサーバ (iRMCSrv)

iRMCSrv では、iRMC S2 が稼働する PRIMERGY サーバのリモートストレージとして使用できる ISO/NRG イメージを作成できます。これは 以下のいずれかで可能となります。

- リモートストレージサーバが稼働するコンピュータ上、または
- マウントされたネットワークドライブ

プロパティ

iRMCSrv リモートストレージサーバは 32 ビットと 64 ビットのバリアントが使用可能で､以下の Linux プラットフォームをサポートします。

– Red Hat Linux 4, Red Hat Linux 5

iRMCSrv リモートストレージサーバは必要に応じて以下のモードで実行することができます。

- バックグラウンドデーモンとして
- スタンドアローンプログラムとして

前提条件

iRMCSrv リモートストレージサーバを使用するには以下の前提条件を満たす必要があります。

- V3.60 以降のファームウェアが稼働する iRMC S2 には V2.0 以降の iRMCSrv リモートストレージサーバが必要です。
- version 3.60 以降のファームウェアが稼働する iRMC S2 は、WinPE 2.**x** に準拠する ISO イメージ、たとえば、Windows サーバ 2008、ServerStart（バージョン 7.1 以降）/Installation Manager、などからブートしなければなりません。

リモートストレージ経由で使用可能な **ISO** イメージの作成

以下の通り進めます。

1. リモートストレージサーバが稼働していることを確認します。
2. Web インターフェースを使用し、リモートストレージ許可がある管理対象サーバの iRMC S2 にログインしてください。
3. 「*Remote Storage* 」ページを使用してリモートストレージサーバの接続を確立してください。

リモートストレージサーバの開始 (iRMCSrv)

以下の通りリモートストレージサーバを開始します。

iRMCSrv [-version] [-daemon] [-port <portnumber>] [<iso-path>]

－バージョン

iRMCSrv のバージョンを表示します。

－デーモン

iRMCSrv をバックグラウンドデーモンとして起動。

－ポート 〈portnumber〉

リモートストレージ接続に使用するポート番号を指定します。
デフォルト： 5901

〈iso-path〉

リモートストレージサーバ上の ISO イメージのパス。

イメージファイルをリモートストレージサーバが稼働しているのコンピュータ以外に置く場合には、イメージファイルのパスを UNC 表記で指定しなければなりません。また、イメージファイルのアクセス権限があるユーザーカウントも必要です。

7 章 iRMC S2 Web インターフェース

iRMC S2 は、それ自身がオペレーティングシステムを持つだけでなく、Web サーバとしても稼動し、そして、それ自身のインターフェースを提供します。iRMC S2 Web インターフェースのメニューおよびダイアログボックスとして、ドイツ語表記と英語表記、日本語表記のいずれかを選択することができます。サーバの種類によりドイツ語が選択できない場合があります。

iRMC S2 Web インターフェースから値を入力するときに、ヒント形式の補助が表示されることがあります。

以下に説明するソフトウェアは、independent JPEG Group の成果に一部基づいています。

7.1 iRMC S2 Web インターフェースへのログイン

➢ リモート管理端末から Web ブラウザを開いて、iRMC S2 の DNS 名（構成されている場合）（ 298 ページ参照）あるいは、IP アドレスを入力してください。

iRMC S2 に LDAP アクセスによるディレクトリサービスが構成されている場合は、別なログイン画面が表示されます（「LDAP 有効」オプションについては、322 ページを参照してください。）：

ログイン画面が表示されない場合は、LAN 接続（LAN インターフェースのテストの 章 37 ページを参照）をチェックしてください。

- iRMC S2 のディレクトリサービスへの LDAP アクセスは、「LDAP 有効」オプションが動作していないときは構築されません。そして、「常に SSL ログイン使用」オプション（322 ページ参 照）は動作しません。

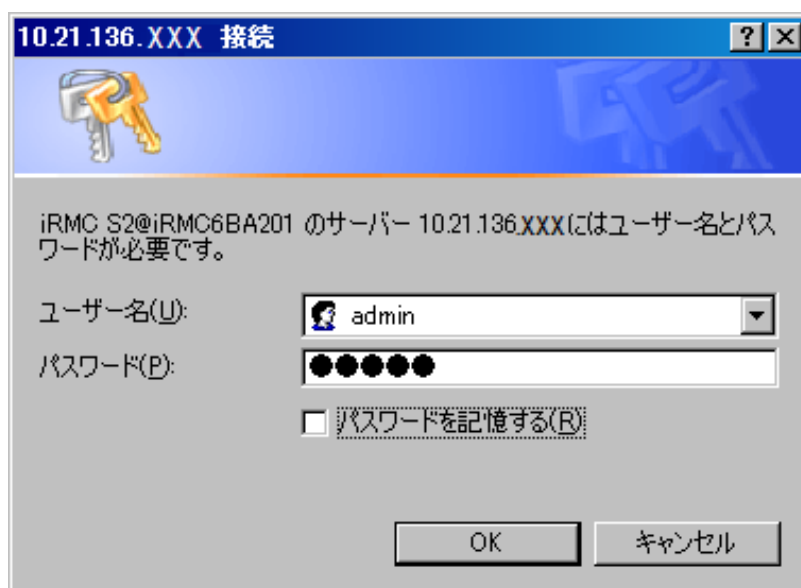



図 92 : iRMC S2 Web インターフェースのログイン画面（LDAP アクセスが構築されておらず、かつ、「常に SSL ログインを使用する」オプションが選択されていない場合）

Ø初期設定の管理アカウントを入力してください。

ユーザー名： admin
パスワード： admin

ユーザー名およびパスワードともに、大文字、小文字を区別します。

安全性の理由から、一度ログインした後は、新しい管理アカウントを作成し、初期設定の管理アカウントを削除するか、少なくともパスワードを変更（314 ページの 「ユーザー名設定－ユーザー設定（詳細）」を参照）するように推奨します。

➢［*OK*］をクリックして、入力を確定してください。

- iRMC S2 の ディレクトリサービスへの LDAP アクセスは、「*LDAP* 有効」オプションが動作しているときに、あるいは「常に *SSL* ログイン使用」オプションが動作しているときに確立します。

FUJITSU
ServerView Suite
PRIMERGY　ServerView® Remote Management iRMC S2 Web Server　English | Deutsch
WIN-TOMOWNBGIY5
継続するにはログインが必要です.
システム情報
iRMC S2
電源制御
電力制御
センサ
システムイベントログ(SEL)
サーバ管理情報
ネットワーク
通知情報設定
ユーザ管理
コンソールリダイレクション
リモートストレージ
iRMC S2 SSH アクセス
iRMC S2 Telnet アクセス
ログアウト
再読み込み
有効なユーザ名とパスワードでログインしてください.
継続するにはログインが必要です
ユーザ名:
パスワード:
安全 (SSL):
ログイン

22-Feb-2010 15:35:41

図 93 : iRMC S2 Web インターフェースのログイン画面（LDAP アクセスが構築されている場合）

ユーザー名およびパスワードは、送信される際、必ず SSL により保護されます。もし、「安全 (SSL)」オプションが動作していれば、web ブラウザと、iRMC S2 間のすべての通信は、HTTPS によって行われます。

Ø初期設定の管理アカウントを入力してください。

ユーザー名：admin

ユーザー名： admin

安全性の理由から、一度ログインした後は、新しい管理者アカウントを作成し、初期設定の管理アカウントを削除するか、少なくともパスワードを変更すること を推奨します（314 ページの「ユーザー名設定－ユーザー設定（詳細）」を参照）。

➢［*ログイン*］をクリックして、ログインを確定してください。

iRMC S2 Web インターフェースの開始は、「システム情報」ページ（219 ページ）を参照してください。

7.2 必要なユーザー許可

表 5 に、iRMC S2 Web インターフェースの各々のファンクションを使用するために必要な許可の概要を示します。

iRMC S2 Web インターフェースのファンクション	IPMI アクセス権限レベルによる許可				必要な許可			
	OEM	管理者	オペレータ	ユーザー	ユーザーアカウントの構成	iRMC S2 設定の構成	ビデオリダイレクション可能	リモートストレージ可能
「System Overview （システム概要）」ページのオープン	?	?	?	?				
識別灯のスイッチオン／オフ	?	?	?	?				
「*Asset Tag Configuration* （アセットタグ設定）」の設定						?		
「System Component Information（システムコンポーネント情報）」 ページのオープン	?	?	?	?				
「*SPD Data* （*SPD データ*）」の表示	?	?	?	?				
「*Reset Error Counter* （*エラーカウンターのリセット*）」						?		
「iRMC S2 Information （iRMC S2 情報）」ページのオープン	?	?	?	?				
「*Reboot iRMC S2* （*iRMC S2 の再起動*）」	?	?						
iRMC S2 へのライセンスキーのアップロード						?		
「 Save iRMC S2 FW Settings （iRMC S2 ファームウェア設定の保存）」ページの編集					?	?		
「*Include User Settings* （*ユーザー設定*）」*の選択*					?			
「*All other Settings* （*その他すべての設定*）」*の選択*						?		
「 Certificate Upload （認証情報のアップロード）」ページのオープンおよび編集						?		
「 Generate a self signed RSA Cert.（自己署名 RSA 認証証明書の作成）」ページのオープンおよび編集						?		
「 iRMC S2 Firmware Update （iRMC S2 ファームウェア更新）」ページのオープン	?	?	?	?				
ファームウェア選択の設定	?	?						
「*Firmware update from file （ファームウェアのファイルからの更新）*」						?		
「*iRMC S2 TFTP using* （*iRMC S2 の TFTP の利用*）」						?		

表 5 : iRMC S2 Web インターフェース利用の許可

iRMC S2 Web インターフェースのファンクション	IPMI アクセス権限レベルによる許可				必要な許可			
	OEM	管理者	オペレータ	ユーザー	ユーザーアカウントの構成	iRMC S2 設定の構成	ビデオリダイレクション可能	リモートストレージ可能
「 iRMC S2 TFTP Firmware Update （TFTP による iRMC S2 ファームウェア更新）」ページのオープンおよび編集						?		
「Power On/Off （電源投入／切断）」ページのオープン	?	?	?	?				
「Boot Options （Boot オプション）」の修正						?		
「Power Control （電源制御）」の利用	?	?	?					
「 Power Options （電源オプション）」ページのオープンおよび編集						?		
「Power Supply Info （電源ユニット情報）」ページのオープン	?	?	?	?				
「 Power Consumption Configuration （消費電力設定）」ページのオープンおよび編集						?		
「 Current Power Consumption （現在のシステム消費電力）」ページのオープン	?	?	?	?				
「 Power Consumption History （消費電力履歴）」ページのオープン*）						?		
「Fan （ファン）」ページのオープン	?	?	?	?				
ファンテストの開始（「Fan Test （ファンテスト）」グループ）	?	?	?	?				
「Fan Check Time （ファンチェック時刻）」の設定（「Fan Test （ファンテスト）」グループ）						?		
各ファンの選択（「System Fans （システムファン）」グループ）						?		
「 Fan Fail Action / Delay Time （ファン故障時の動作／待機時間）」の設定						?		
「Temperature （温度）」ページのオープン	?	?	?	?				
危険温度時の動作定義						?		
「Voltages （電　圧）」ページのオープン	?	?	?	?				
「Power Supply （電源ユニット）」ページのオープン	?	?	?	?				
「 Component Status （コンポーネントの状態）」ページのオープン	?	?	?	?				
「 System Event Log Content （システムイベントログの内容）」ページのオープン	?	?	?	?				
システムイベントログのクリア（選択）	?	?	?					
「Save event log （イベントログの保存）」	?	?	?	?				

表 5 : iRMC S2 Web インターフェース利用の許可

iRMC S2 Web インターフェースのファンクション	IPMI アクセス権限レベルによる許可				必要な許可			
	OEM	管理者	オペレータ	ユーザー	ユーザーアカウントの構成	iRMC S2 設定の構成	ビデオリダイレクション可能	リモートストレージ可能
画面への選択入力の厳格度の定義	?	?	?	?				
「System Event Log Configuration（システムイベントログの設定）」ページのオープン	?	?	?	?		?		
「System Event Log Configuration（システムイベントログの設定）」ページのオープンおよび編集						?		
「Server Management Info（サーバ管理情報）」ページのオープンおよび編集						?		
「Network Interface（ネットワークインターフェース）」ページのオープンおよび編集						?		
「Ports and Netw. Services（ポート番号およびネットワークサービス）」ページのオープンお						?		
「DHCP Configuration（DHCP 構成）」ページのオープンおよび編集						?		
「DNS Settings（DNS 設定）」ページのオープンおよび編集						?		
「SNMP TRAP Alerting（SNMP トラップ警告通知）」ページのオープンおよび編集						?		
「Serial / Modem Alerting（シリアル／モデム警告通知）」ページのオープンおよび編集						?		
「Email Alerting（E-mail 警告通知）」ページのオープンおよび編集					?	?		
「iRMC S2 User（iRMC S2 ユーザー）」ページのオープンおよび編集								
「Directory Service Config.（ディレクトリサービス設定）」ページのオープンおよび編集						?		
「BIOS Text Console（BIOS テキストコンソール）」ページのオープン	?	?	?	?				
「BIOS Console Redirection Options（BIOS コンソールリダイレクションオプション）」の修正						?		
「Start Console Redirection（コンソールリダイレクションの開始）」	?	?	?	?				
電源制御およびテキストコンソールへの「Logon（ログオン）」	?	?						
テキストリダイレクションの開始（「Enter Console（コンソール入力）」）	?	?						
「Adv. Video Redirection（ビデオリダイレクション）」ページのオープンおよび編集							?	
「Remote Storage（リモートストレージ）」ページのオープンおよび編集								?
「iRMC S2 SSH Access（iRMC S2 への SSH アクセス）」の開始	?	?	?	?				
SSH ログイン	?	?	?	?				

表 5 : iRMC S2 Web インターフェース利用の許可

iRMC S2 Web インターフェースのファンクション	IPMI アクセス権限レベルによる許可				必要な許可			
	OEM	管理者	オペレータ	ユーザー	ユーザーアカウントの構成	iRMC S2 設定の構成	ビデオリダイレクション可能	リモートストレージ可能
「 iRMC S2 Telnet Access （iRMC S2 への TELNET によるアクセス）」の開始	?	?	?	?				
Telnet ログイン	?	?	?	?				

*） これは、一部の PRIMERGY サーバではサポートされていません。

表 5 : iRMC S2 Web インターフェース利用の許可

7.3 ユーザーインターフェース画面

iRMC S2 Web インターフェースの画面を以下に示します。

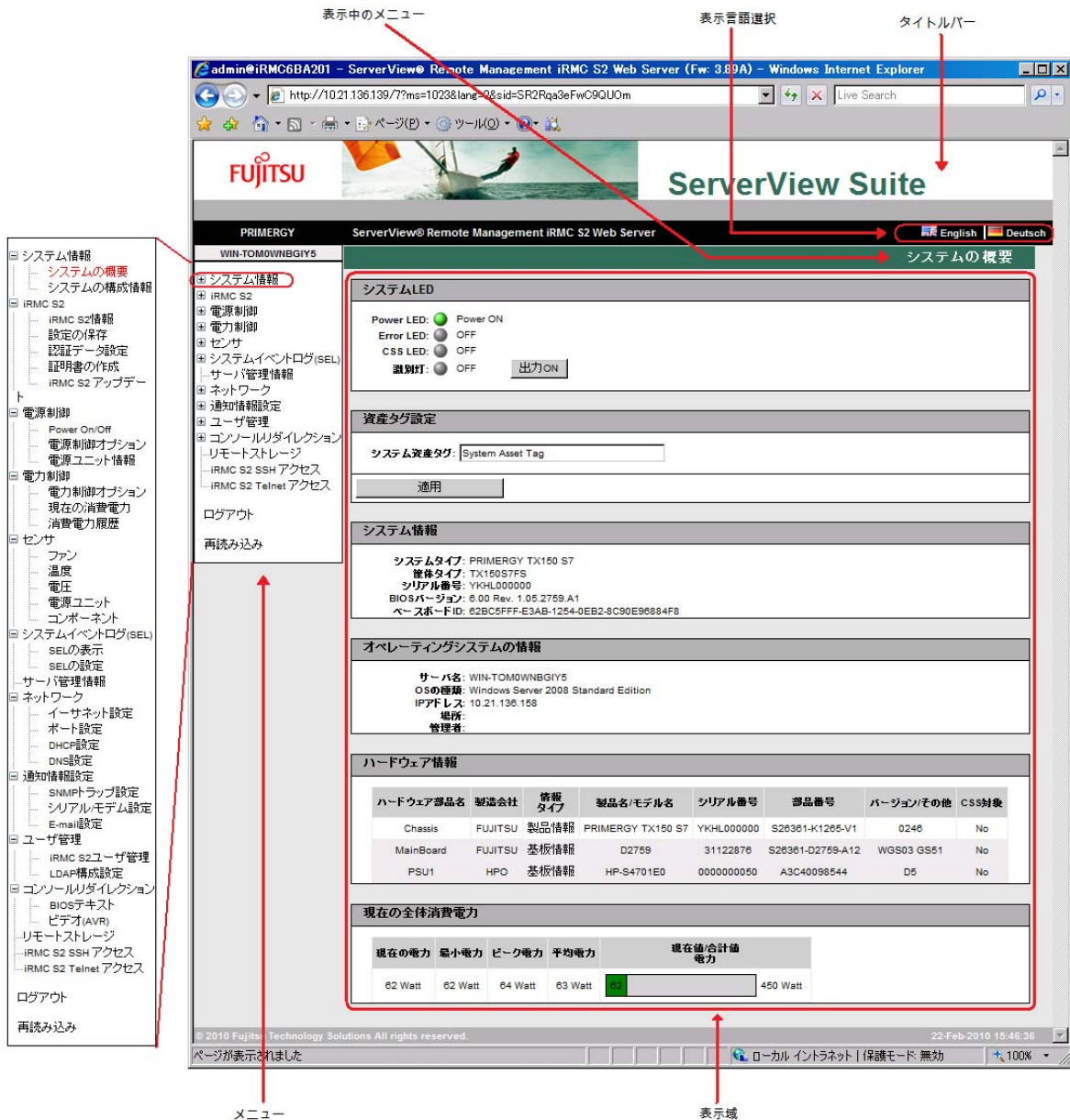



図 94 : iRMC S2 Web インターフェース画面

iRMC S2 Web インターフェースの言語の選択

ワークエリアの上の黒いバーの右に、旗のアイコンがあります。このアイコンをクリックして、iRMC S2 Web インターフェースのナビゲーションエリア、メニューおよびダイアログボックスを表示する言語（ドイツ語、英語あるいは日本語）を選択してください。

ナビゲーションエリア

ナビゲーションエリアは、iRMC S2 の個々の機能をタスクベースに並べたメニューツリーの構造を含んでいます（図 94 ：「システム概要」参照）。これらのリンクの中から 1 つをクリックすると、その リンクが有効になり、その機能の出力、ダイアログボックス、オプション、リンクおよびボタンがワークエリアに表示されます。
個々の iRMC S2 の機能の下に、［ログアウト］および［再読み込み］のリンクがあります。

- ［ログアウト］は、ダイアログボックスでの確認の後、iRMC S2 のセッションを終了させることができます。iRMC S2 に LDAP アクセスによるディレクトリサービスが構成されている場合は、別のログイン画面が表示されます（「LDAP 有効」オプションについては、322 ページを参照してください）。

  - iRMC S2 の ディレクトリサービスへの LDAP アクセスは、「LDAP 有効」オプションが動作していないときは確立しません。また、「常に *SSL* ログイン使用」オプション（322 ページ参照）無効の場合は、次の画面が表示されます。

図 95 ：ログインページ（ログアウト後）

［ログイン］ボタンをクリックして、iRMC S2 Web インターフェースのログイン画面をオープンしてください。画面は、（図 92 ）を参照してください。再びログインすることができます。

- iRMC S2 用に LDAP ディレクトリサービスが構成されている場合（「*LDAP* 有効」オプションが動作している場合）、あるいは、「常に *SSL* ログイン使用」オプション（210 ページ参照）が動作していない場合は、それに応じたログイン画面が表示されます（図 93 を参照）。

● ［再読み込み］ボタンをクリックすると、iRMC S2 Web インターフェースの内容を再読み込みすることができます。

> i ［再読み込み］ボタンをクリックする代わりに、Web インターフェースの自動更新を設定することもできます。Web インターフェースの内容が周期的に再読み込みされます（294 ページの「自動再読み込みの有効」を参照してください）。

7.4 システム情報－サーバ上の情報

「システム情報」の内容は、次のページに含まれています :

- 220 ページの「システム概要－サーバ上の一般情報」
- 225 ページの「システム構成情報－サーバの構成情報」

7.4.1 システム概要 – サーバ上の一般情報

「システム概要」ページでは、次の情報を提供します。

－システムの状態

－システム（一般的な情報）

－管理サーバのオペレーティングシステム

－システム FRU （取替え可能ユニット）/IDPROM.

－管理サーバの現状の電源消費の総合情報

「システム概要」ページでは、上記の情報の表示に加え、管理サーバに顧客特有の資産タグを入力することができます。

図 96 ：システム概要ページ

システム状態

Error LED、CSS LED および識別灯は、「システム状態」として以下のように表示されます。PRIMERGY の識別灯のオン／オフもできます。

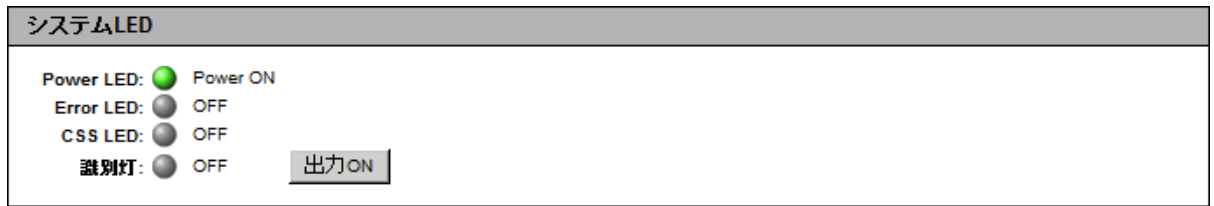



図 97 ：システム概要ページーシステム状態

「 *Power LED*」

サーバの電源状態を示します。
次の状態を示します：

－オン： RAM へのサスペンド（スタンバイ）という文字と一緒に電源オン（緑）
－オン： RAM へのサスペンド（スタンバイ）という文字と一緒にスタンバイモード（緑）
－オフ：電源オフ（オレンジ）

「 *Error LED* 」

サーバの Error LED 情報：

ステータス情報 （**iRMC S2**）	サーバの **Error LED**	サーバの状態
オフ	光らない。	危機的イベントなし。
オン	赤く点灯する。	CSS 部品ではないコンポーネントの故障の前兆あり。
点滅	赤く光る。	危機的状態にあり。

「 *CSS LED* 」

サーバの CSS LED 情報：

ステータス情報 （**iRMC S2**）	サーバの **CSS LED**	サーバの状態
オフ	光らない。	サーバは稼動中。
オン	オレンジに点灯する。	CSS 部品の故障の前兆あり。
点滅	オレンジに光る。	CSS 部品の故障あり。

「*識別灯*」
サーバの状態を表示します。
次の状態を示します：

－オン（青）
－オフ（灰色）

「オン／オフ」
［オン／オフ］ボタンで、PRIMERGY の識別灯をオン／オフしてください。

資産タグ構成

「資産タグ設定」で、管理サーバに顧客特有の資産タグを入力することができます。

i 顧客特有の資産タグで、サーバに番号を付けたり、その他の識別子をつけることができます。

ウィンドウズベースのシステムでは、この顧客特有の資産タグは、自動的に WMI で供給されます。資産タグは、社内ツールで利用されたり、企業管理システム (CA Unicenter など) の統合に利用されたりします。

資産タグ設定

システム資産タグ: System Asset Tag

適用

図 98 ：システム概観ページ － システム状態

「システム資産タグ」
ここに資産タグを入力します。

➤［*適用*］をクリックして、資産タグを適用させてください。

システム情報

「システム情報」は、管理サーバの情報を表示します。

システム情報

システムタイプ:	PRIMERGY TX150 S7
筐体タイプ:	TX150S7FS
シリアル番号:	YKHL000000
BIOSバージョン:	6.00 Rev. 1.05.2759.A1
ベースボードID:	62BC5FFF-E3AB-1254-0EB2-8C90E96884F8

図 99 ：システム概要ページーシステム情報

オペレーティングシステム情報

「オペレーティングシステム情報」は、管理サーバのオペレーティングシステムの情報を表示します。

オペレーティングシステムの情報

サーバ名:	WIN-TOM0WNBGIY5
OSの種類:	Windows Server 2008 Standard Edition
IPアドレス:	10.21.136.XXX
場所:	
管理者:	

図 100 ：システム概要ページーオペレーティングシステム情報

ハードウェア情報

フィールド交換ユニットの情報が「ハードウェア情報」の下に表示されます。システム交換ユニットとは、システムから取り外して交換できる部品を指します。「**CSS** 対象」列は、それぞれの部品が顧客自己保守機能をサポートしているか否かを表しています。

オペレーティングシステムの情報

サーバ名: WIN-TOM0WNBGIY5
OSの種類: Windows Server 2008 Standard Edition
IPアドレス: 10.21.136.XXX
場所:
管理者:

図 101 ：システム概要ページーハードウェア情報

現在の全体消費電力

このオプションは、一部の **PRIMERGY** サーバではサポートされていません。

現在の全体消費電力

現在の電力	最小電力	ピーク電力	平均電力	現在値/合計値電力
62 Watt	62 Watt	63 Watt	62 Watt	62 450 Watt

図 102 : システム概要ページー現在の全体消費電力

「現在の全体消費電力」の下に、設定された間隔で測定されたサーバの消費電力量の現在値、最小値、最大値、平均値を表示しています。

グラフィカルな表示は、サーバの可能な最大消費電力量と現在の消費電力量を比較して表示しています。

7.4.2 システム構成情報 – サーバの構成情報

「システム構成情報」ページは、CPU およびメインメモリモジュールの情報を提供します。「CSS 対象」列は、それぞれのコンポーネントが顧客自己保守機能をサポートしているか否かを表しています。

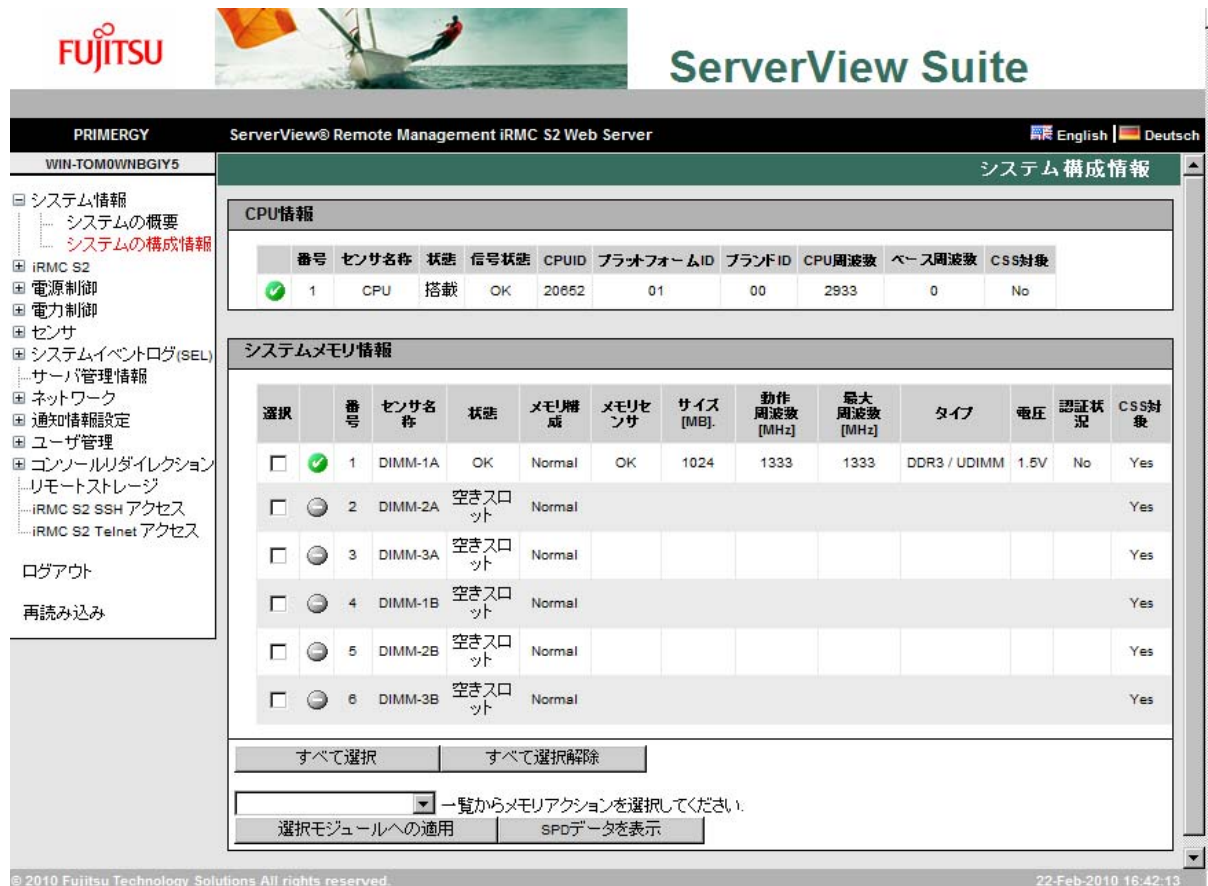
以下のステータスアイコンは、各監視センサの状態を示しています：

	OK ：コンポーネントの状態は良好です。
	コンポーネントのスロットが空の状態です。
	警告：コンポーネントの状態が低下しています。
	欠陥：コンポーネントに欠陥があります。

表 6 : 各監視センサの状態

図 103 ：システム構成情報ページ

PRIMERGY サーバは、TPM(Trusted Platform Module) をサポートしています。このページは、TPM を動作させるか、停止させるかを設定します。

システム CPU 情報

このグループでは、PRIMERGY サーバの CPU の状態 ID、CSS 能力および性能の情報を提供します。

システムメモリ情報

このグループでは、PRIMERGY サーバのメインメモリモジュールの状態、ID、CSS 能力および性能の情報を提供します。

「*選択*」
稼動させるメモリモジュールを「一覧からメモリアクションを選択してください」リストから選択してください。

［*すべて選択*］
すべてのメモリモジュールを選択します。

［すべて選択解除］
［すべて選択解除］

「一覧からメモリアクションを選択してください」
このリストから選択されたメモリモジュールが稼動します。

このリストから選択されたメモリモジュールが稼動します。
選択されたメモリモジュールを適用します。

［*SPD* データを表示］
［SPD データを表示］ボタンを切り替えて、ベンダー特有の個々のメモリの情報 (Serial Presence Detect(SPD) 情報）の表示／非表示を切り替えてください。

メモリの SPD データは、EEPROM に保存され、コンポーネントおよびサーバに連携されて、BIOS が自動的にメモリの検出（RAM、DIMM）を行うことを許可します。

7.5 iRMC S2 －情報、ファームウェアおよび認証

「 *iRMC S2* 」の内容は、次のページに含まれています：

- 229 ページの「iRMC S2 情報－ iRMC S2 に関する情報」
- 233 ページの「 iRMC S2 ファームウェア設定の保存－ファームウェア設定の保存」
- 235 ページの「認証情報のアップロード－ DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード」
- 242 ページの「自己署名証明書の作成－自己署名 RSA 証明書の作成」
- 244 ページの「 iRMC S2 ファームウェアの更新」

7.5.1 iRMC S2 情報 – iRMC S2 に関する情報

「iRMC S2 情報」ページは、以下のオプションを提供します。

- ファームウェア情報、iRMC S2 の SDRR バージョンの表示、ファームウェアの選択、ファームウェアイメージのロード、および、iRMC S2 の再起動
- 動作中の iRMC S2 セッションに関する情報の表示
- 動作中の iRMC S2 セッションに関する情報の表示

図 104 : iRMC S2 情報ページ

動作中ファームウェア

「動作中ファームウェア」の下に、iRMC S2 のファームウェアおよび SDRR バージョン情報が表示され、iRMC S2 を再起動することができます。

動作中ファームウェア

iRMCバージョン: 3.89A
ファームウェア作成日: Jan 22 2010 - 07:36:30
動作中ファームウェア: ファームウェア1
ハードウェアバージョン: 2 Chip ID: 8A C4 44 16 49 13 60
SDRRバージョン: 3.08 ID 0246 TX150S7

iRMC S2を再起動

図 105 : iRMC S2 情報ページーファームウェア情報および iRMC S2 の再起動

［*iRMC S2* を再起動］
iRMC S2 を再起動します。

［*iRMC S2* を再起動］ボタンは、管理サーバの BIOS POST フェーズでは、使用できません。

実行中のセッション情報

「実行中のセッション情報」グループは、iRMC S2 のすべての実行中のセッションを表示します。

実行中のセッション情報

IPアドレス	ユーザ名	ユーザID	接続プロトコル	アクセス権限	アクセス形態	リモートポート
10.17.192.XXX	admin	2	HTTP	OEM	Web GUI	49941
10.21.136.YYY	admin	2	HTTP	OEM	Web GUI	0

図 106 : **iRMC S2** 情報ページー実行中のセッション情報

ライセンスキー

「ライセンスキー」グループで、iRMC S2 にライセンスキーをアップロードすることができます。

実行中のセッション情報

IPアドレス	ユーザ名	ユーザID	接続プロトコル	アクセス権限	アクセス形態	リモートポート
10.17.192.XXX	admin	2	HTTP	OEM	Web GUI	49941
10.21.136.YYY	admin	2	HTTP	OEM	Web GUI	0

図 107 : iRMC S2 情報ページーライセンスキー

iRMC S2 の機能を利用するには正式なライセンスキーが必要です（「ビデオリダイレクション」（344 ページ参照）および「リモートストレージ」（354 ページ参照））。

ライセンスキーを購入することができます。

［アップロード］
このボタンをクリックすると、ライセンスキーが iRMC S2 にアップロードされます。

iRMC S2 その他のオプション

「*iRMC S2* その他のオプション」グループで、iRMC S2 Web インターフェースのレイアウトを設定することができます。

iRMC S2 その他のオプション	
デフォルト言語:	日本語
温度単位:	摂氏温度
デザイン:	スタイルガイド Version 2
適用	

図 108 : iRMC 情報ページー iRMX S2 その他のオプション

「*デフォルト言語*」
言語（ドイツ語／英語／日本語）の初期設定を設定します。次回 iRMC S2 Web インターフェースを呼び出す際に有効になります。

「温度単位」
iRMC S2 Web インターフェースで表示する温度の単位（摂氏／華氏）を設定します。この設定は、次回 iRMC S2 Web インターフェースを呼び出す際に有効になります。

「*デザイン*」
iRMC S2 Web インターフェースに表示するカラースキーマを設定します。この設定は、次回 iRMC S2 Web インターフェースを呼び出す際に有効になります。

7.5.2 iRMC S2 ファームウェア設定の保存 – ファームウェア設定の保存

「***iRMC S2*** ファームウェア設定」ページで、現在のファームウェア設定および iRMC S2 の他の設定をファイルに保存することができます。

- 「*iRMC S2* ファームウェア設定を *ServerView* の *XML* 形式で保存」下で選択されたファームウェア設定が、*iRMC_S2_settings.pre* というファイル名で保存されます。WinSCU については、391 ページを参照してください。［インポート］ボタンで、ファームウェア設定を iRMC に再びアップロードすることができます。

- 「iRMC S2 ファームウェア設定をバイナリ (*BMCCLONE.exe*) で保存」下で選択されたファームウェア設定が、*iRMC_S2_settings.bin* というファイル名で保存されます。

注意！
必ず、「iRMC S2 ファームウェア設定を ServerView の XML 形式で保存」を使って設定の保存を行ってください。
「*iRMC S2* ファームウェア設定をバイナリ（*BMCCLONE.exe*）で保存」は、管理サーバのシステムモジュールを入れ替える場合のみ使用してください。

i ユーザー設定を保存する場合は、「ユーザー設定」アクセス権限を持つ「ユーザー カウントの設定」を行ってください。すべての場合において、「iRMC S2 設定の構成」アクセス権限で十分です。

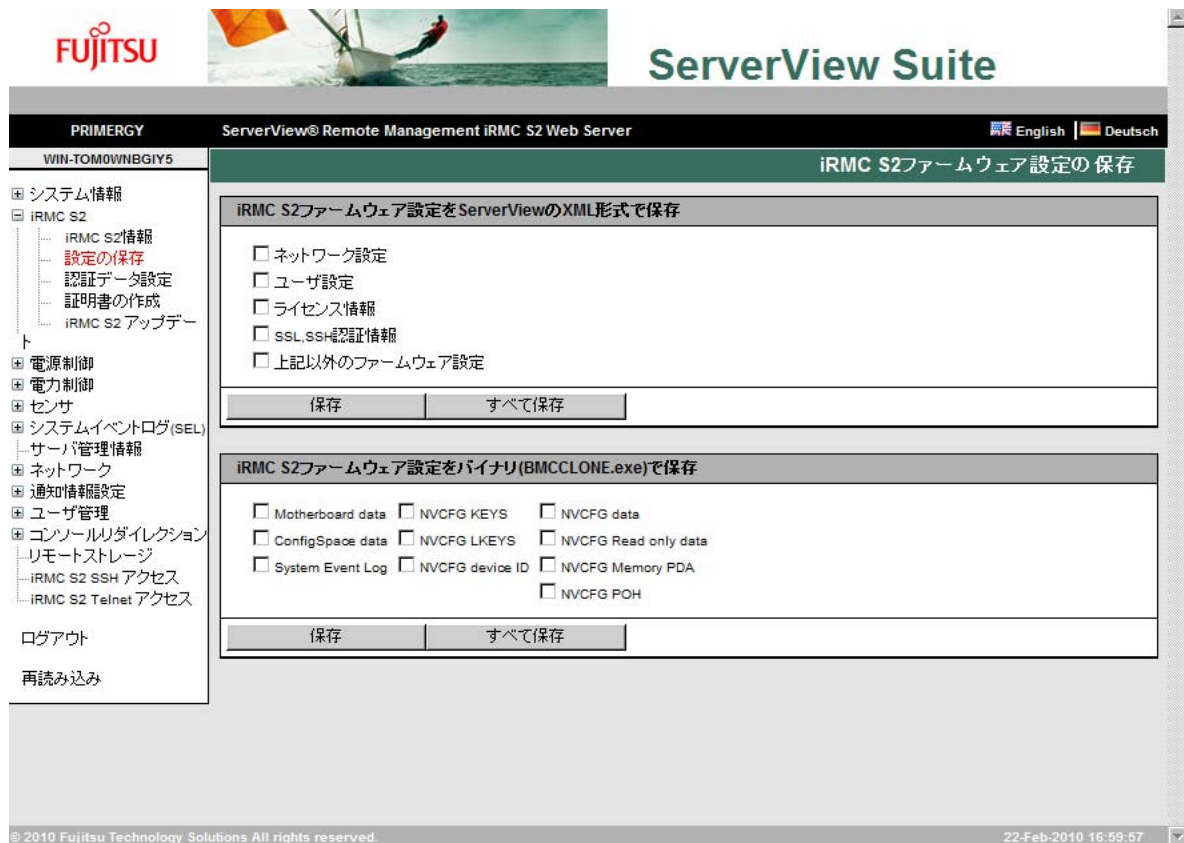



図 109 : iRMC S2 ファームウェア設定

［*保存*］

選択した設定を保存するには、［保存］をクリックしてください。

［*すべて保存*］

すべての設定を保存するには、［すべて保存］をクリックしてください。

7.5.3 認証情報のアップロード – DSA/RSA 証明書および DSA/RSA 秘密鍵のアップロード

「*認証情報のアップロード*」ページで、認証機関 (CA) からの署名付 X.509 DSA/RSA 証明書 (SSL)、あるいは、DSA/RSA 秘密鍵 (SSH) を iRMC S2 にアップロードすることができます。

iRMC S2 は、あらかじめ定義されたサーバ認証証明書（規定の証明書）を提供します。もし、セキュアな SSL/SSH で、iRMC S2 に接続したい場合、認証機関 (CA) からの署名付認証証明書にできるだけ早く置き換えることを推奨します。

X.509 DSA/RSA 認証および DSA/RSA 秘密鍵の入力フォーマット：

X.509 DSA/RSA 証明書および RSA/DSA 秘密鍵は、共に、PEM エンコードフォーマット (ASCII / Base64) に対応していなければなりません。

図 110：認証情報のアップロードページ

現在の有効な DSA/RSA 認証局証明書の表示

- 「*証明書の情報とリストア*」グループの［Web 証明書を表示］をクリックすると、現在の有効な証明書の情報を表示します。
- 「*証明書の情報とリストア*」グループの［認証局の証明書を表示］をクリックすると、現在の有効な認証局証明書を表示します。

図 111 ：証明情報のアップロードページ－現在 SSL/SSH 証明書

規定の証明書および規定の認証局証明書のリストア

➢「証明書の情報とリストア」グループの［規定の証明書に戻す］をクリックすると、規定の証明書がファームウェアに設定されます。

➢「証明書の情報とリストア」グループの［規定の認証局証明書に戻す］をクリックすると、規定の認証局証明書がファームウェアに設定されます。

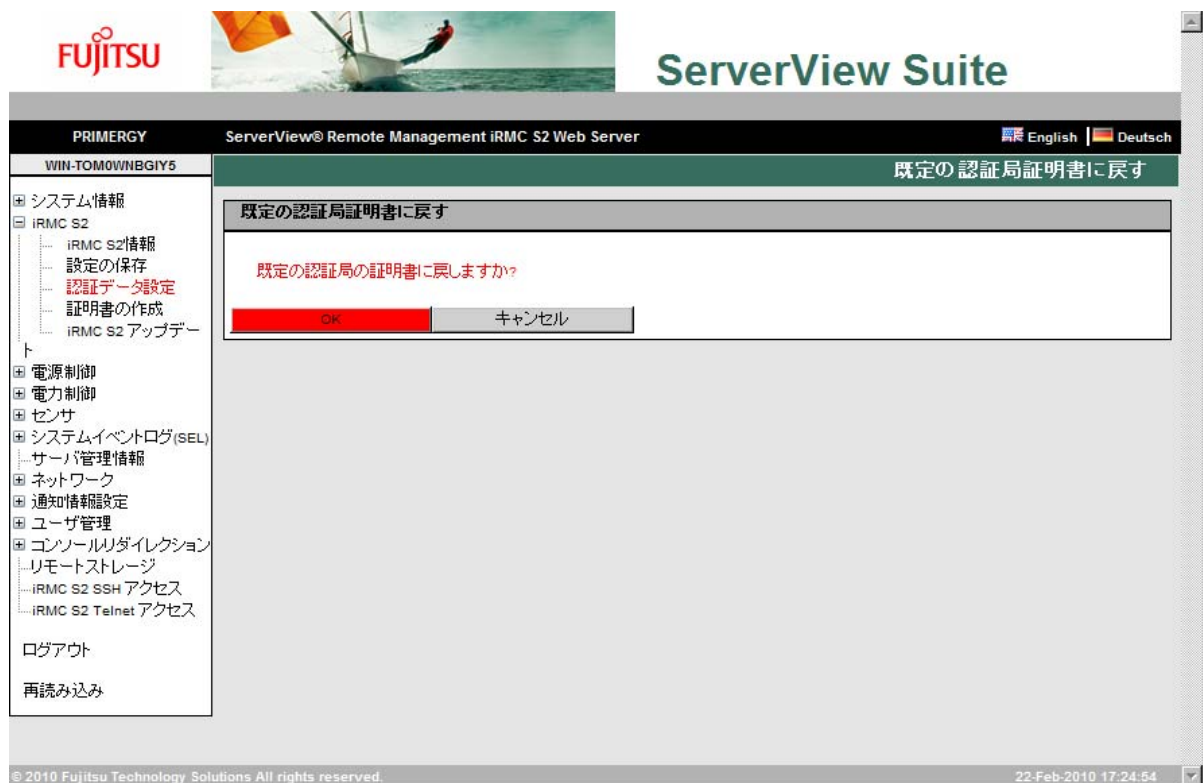



図 112 ：証明書のアップロードページー規定の認証局証明書に戻す

認証局証明書ファイルのアップロード

「認証局証明書ファイルのアップロード」グループを使って、認証局証明書をローカルファイルから登録することができます。

認証局証明書ファイルのアップロード

注:ローカルファイルよりbase64(PEM)エンコードされたX.509認証局証明書をアップロードします.
ファイルのアップロード後、すべてのhttps接続は切断され、httpsサーバが自動的に再起動されます.この作業は最大30秒ほどかかり
iRMC S2のリセットは要求されません.

認証局証明書ファイル: 参照...

アップロード

図 113：認証局証明書のアップロード

次の手順で行ってください：

- 管理サーバ上のローカルファイルに認証局証明書を保存してください。
- 「認証局証明書ファイル」ページ内の［参照］ボタンをクリックして、認証局証明書を含んだファイルを選択してください。
- ［アップロード］ボタンをクリックして、認証局証明書あるいは秘密鍵を iRMC S2 に登録してください。

> **i** 認証局証明書あるいは秘密鍵を登録すると、すべての HTTPS 接続は切断され、HTTPS サーバが自動的に再起動します。これには、30 秒ほどかかります。iRMC S2 のリセットは必要ありません。

- ［認証局証明書を表示］ボタンをクリックして、認証局証明書の登録が成功していることを確認してください。

SSL 証明書と DSA/RSA 秘密鍵ファイルのアップロード

「**SSL** 証明書と **DSA/RSA** 秘密鍵ファイルのアップロード」グループを使って、行うことができます。

i 秘密鍵と証明書は、**iRMC S2** に同時にアップロードされなければなりません。

SSL証明書とDSA/RSA秘密鍵ファイルのアップロード

注: base64(PEM)エンコードされたX.509証明書、および DSA/RSA 秘密鍵をローカルファイルからアップロードします.
重要:両ファイルは続けてアップロードする必要があります.
ファイルのアップロード後、すべてのhttps接続は切断され、httpsサーバが自動的に再起動されます.この作業は最大30秒ほどかかり
iRMC S2のリセットは要求されません.

秘密鍵ファイル: [参照...]
証明書ファイル: [参照...]

[アップロード]

図 114 : **SSL** 証明書と **DSA/RSA** 秘密鍵ファイルのアップロード

次の手順で行ってください :

- **X.509 DSA/RSA(SSL)** 証明書および **DSA/RSA** 秘密鍵を管理サーバ上のそれぞれのローカルファイルに保存してください。
- 「秘密鍵ファイル」および「証明書ファイル」ページ内の［参照］ボタンをクリックして、秘密鍵あるいは証明書ファイルを選択してください。
- ［アップロード］ボタンをクリックして、証明書あるいは秘密鍵を **iRMC S2** に登録してください。

  i 証明書あるいは秘密鍵を登録すると、すべての **HTTPS** 接続は切断され、**HTTPS** サーバが自動的に再起動します。これには **30** 秒ほどかかります。**iRMC S2** のリセットは必要ありません。

- ［***Web*** 証明書を表示］ボタンをクリックして、証明書の登録が成功していることを確認してください。

コピー&ペーストで **SSL DSA/RSA** 証明書、および **DSA/RSA** 秘密鍵をアップロード

「コピー&ペーストで **SSL DSA/RSA** 証明書、および **DSA/RSA** 秘密鍵をアップロード」グループを使って、行うことができます。

この方法は、**iRMC S2** に **root** アクセス権限の証明書を登録する場合には使わないでください。**root** アクセス権限の証明書を登録する場合はファイルによる方法を使ってください。(240 ページ参照)

コピー&ペーストでのSSL DSA/RSA証明書、およびDSA/RSA秘密鍵をアップロード

注:ファイルの代わりに、base64(PEM)エンコードされたX.509 SSL証明書、またはDSA/RSA 秘密鍵コンテンツを以下のテキストボックスに貼り付けてアップロードできます.
重要:両ファイルは続けてアップロードする必要があります.
重要:この方法で証明局認証書をiRMC S2へアップロードしないでください.ファイルからのアップロードをお願いします.
重要:下記テキストボックスへファイルを貼り付けアップロードした後、iRMC S2を手動で再起動する必要があります.

アップロード

図 115 : コピー&ペーストで **SSL DSA/RSA** 証明書、および **DSA/RSA** 秘密鍵をアップロード

次の手順で行ってください :

➢ 入力エリアに、**X.509 DSA** 証明書あるいは **DSA** 秘密鍵をコピーしてください。

認証書および秘密鍵を同時に入力することはできません。

➢ [アップロード] ボタンをクリックして、証明書あるいは秘密鍵を **iRMC S2** に登録してください。
➢ リモートマネジメントを使って、**iRMC S2** をリセットしてください (379 ページの「サービスプ ロセッサー IP パラメータ、診断用 LED 、および、iRMC S2 のリセット」の章を参照)

これは、**iRMC S2** に登録した証明書および秘密鍵を有効にするために必要です。

➢ [***Web*** *証明書を表示*] ボタンをクリックして、証明書の登録が成功していることを確認してください。

7.5.4 自己署名証明書の作成 – 自己署名 RSA 証明書の作成

「自己署名 ***RSA*** 証明書の作成」ページを使って、自己署名証明書を作成することができます。

図 116 : 自己署名証明書の作成ページ

証明書の情報とリストア

「証明書の情報とリストア」グループを使って、現状の有効な **DSA/RSA** 証明書の表示あるいは規定の **RSA/DSA** 証明書をリストアすることができます。

［***Web*** *証明書を表示*］
このボタンを使って、現状の有効な **DSA/RSA** 証明書を表示することができます。

［*規定の証明書に戻す*］
このボタンを使って、確定後、規定の証明書をファームウェアにリストアすることができます。

証明書の作成

次の手順で、自己署名証明書を作成することができます：

➤「*証明書の作成*」の下に詳細な必要項目を入力してください。

➤［*作成*］をクリックして、証明書を作成してください。

i 新しい証明書を生成すると、すべての **HTTPS** 接続は切断され、**HTTPS** サーバが自動的に再起動します。
キーの長さによって、**5** 分程度かかります。**iRMC S2** のリセットは必要ありません。

7.5.5 iRMC S2 ファームウェアアップデート

「*iRMC S2* ファームウェアアップデート」ページを使って、**iRMC S2** ファームウェアをオンラインで更新することができます。これを行うためには、更新するファームウェアイメージをリモート管理端末のローカルあるいは **TFTP** サーバ上に配置しなければなりません。

ここでは、**iRMC S2** ファームウェアおよびファームウェア選択に関する情報も参照してください。

図 117： **iRMC S2** ファームウェアアップデートページ

ファームウェア情報

「*ファームウェア情報*」の下に、**iRMC S2** のファームウェアおよび **SDRR** バージョン情報が表示され、ファームウェアを選択することができます。

ファームウェア	起動プログラム	ファームウェアバージョン	SDRRバージョン	SDRR ID	チェックサム	状態
ファームウェア1	3.09	3.89A	3.08	0246	OK	動作中
ファームウェア2	3.09	3.88A	3.07	0246	OK	不活性

図 118 : **iRMC S2** ファームウェアアップデートーファームウェア情報

「*ファームウェア変更*」

次回 **iRMC S2** を再起動するときに、有効にするファームウェアを選択することができます。

次のオプションがあります :

- 「自動ー版数が新しいファームウェアを使用」
  ファームウェアは、自動的に最新のバージョンが選択されます。
- 「ファームウェア **1**」
  ファームウェアエリア **1** のファームウェアが選択されます。
- 「ファームウェア **2**」
  ファームウェアエリア **2** のファームウェアが選択されます。
- 「版数が古いファームウェアを選択」
  最も古いバージョンのファームウェアが選択されます。
- 「書込日が新しいファームウェア」
  書き込まれた日時が新しいファームウェアが選択されます。
- 「書込日が古いファームウェア」
  書き込まれた日時が古いファームウェアが選択されます。

［*適用*］

［*適用*］をクリックして、「ファームウェア変更」に設定されたファームウェアを設定してください。

ファイルからのファームウェアアップデート

「ファイルからのファームウェアアップデート」ページを使って、**iRMC S2** ファームウェアをオンラインで更新することができます。これを行うためには、更新するファームウェアをリモート管理端末のファイルに配置しておかなければなりません。

適切なファームウェアが、**PRIMERGY** サーバの **ServerView Suite DVD 1** 、あるいは、以下の **URL** からダウンロードすることができます。

http://support.ts.fujitsu.com/com/support/downloads.html

ファイルからのファームウェア アップデート	
Flash書込先の選択:	自動 - 不活性なファームウェア
アップデート ファイル:	参照...
適用	

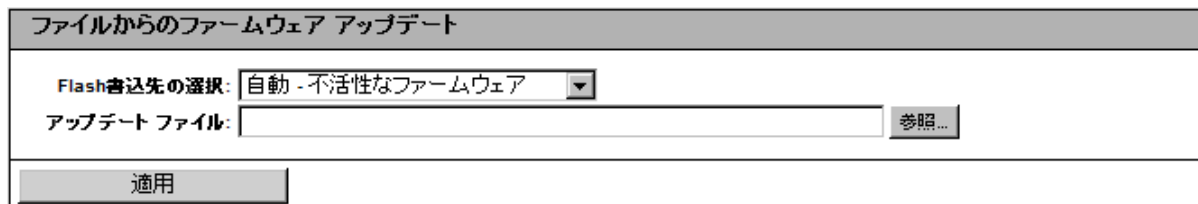



図 119 : **iRMC S2** ファームウェア更新ページーファイルからのファームウェアアップデート

「Flash 書込先の選択」

iRMC ファームウェア更新に使用します。
次のオプションがあります：

- 「*自動－不活性なファームウェア*」
  不活性なファームウェアが自動的に選択されます。
- 「*ファームウェア **1***」
  ファームウェアエリア **1** のファームウェアが選択されます。
- 「*ファームウェア **2***」
  ファームウェアエリア **2** のファームウェアが選択されます。

「*アップデートファイル*」
ファームウェアが保存されたファイルを設定します。

以下のリストされたファイルについて、毎回更新（実行用ファームウェアおよび SDR レコード）が実行されるたびに、iRMC S2 ファームウェア構成が、それぞれ更新されます。

rt_sdt_<D-number>_4_08g_00.bin ファイルは、いくつかの PRIMERGY サーバあるいはブレードサーバにも利用可能です。これにより、iRMC S2 ファームウェアのすべての更新を一度の操作で行うことができます。

「*dcod<FW-Version>.bin*」
ファームウェアの実行版を更新します。

「*<SDR-Version>.SDR*」
SDR レコードを更新します。

［*参照*］
ファイルブラウザを開いて、更新ファイルを選択できるようにします。

➢ ［*適用*］ボタンをクリックして、iRMC S2 ファームウェアの設定および更新を開始してください。

iRMC S2 TFTP 設定

「ファイルからのファームウェアアップデート」ページを使って、iRMC S2 ファームウェアをオンラインで更新することができます。これを行うためには、更新するファームウェアをリモート管理端末のファイルに配置しておかなければなりません。

適切なファームウェアが、PRIMERGY サーバの ServerView Suite DVD 1 、あるいは、以下の URL からダウンロードすることができます。

http://support.ts.fujitsu.com/com/support/downloads.html

図 120 ： iRMC S2 ファームウェア更新ページ － iRMC S2 TFTP 設定

「*TFTP サーバ*」
ファームウェアのファイルが保存された TFTP サーバの IP アドレスあるいは DNS 名を設定します。

「*アップデートファイル*」

ファームウェアが保存されたファイルを設定します。

以下のファイルについて、毎回 TFTP サーバを利用した更新（実行用ファームウェアおよび SDR レコード）が実行されるたびに、iRMC S2 ファームウェア構成が、それぞれ更新されます。

rt_sdt_<D-number>_4_08g_00.bin ファイルは、いくつかの PRIMERGY サーバあるいはブレードサーバにも利用可能です。これにより、TFTP サーバを使って、iRMC S2 ファームウェアのすべての更新を一度の操作で行うことができます。

「*dcod<FW-Version>.bin*」

ファームウェアの実行版を更新します。

「*<SDR-Version>.SDR*」

SDR レコードを更新します。

「*Flash* 書込先の選択」

iRMC ファームウェア更新に使用します。
次のオプションがあります：

- 「自動－不活性なファームウェア」

  不活性なファームウェアが自動的に選択されます。
- 「ファームウェア 1」

  ファームウェアエリア 1 のファームウェアが選択されます。
- 「ファームウェア 2」

  ファームウェアエリア 2 のファームウェアが選択されます。

➢［適用］ボタンをクリックして、設定を有効にしてください。

➢［TFTP テスト］ボタンをクリックして、TFTP サーバとの接続をテストしてください。

➢「TFTP 開始」ボタンクリックして、TFTP サーバからファームウェアを含んだファイルをダウンロードし、iRMC S2 ファームウェアの更新を開始してください。

7.6 Power Management

Power Management エントリは、PRIMERGY サーバの電源管理ページのリンクを含みます。

- 250 ページの「 Power ON/OFF －サーバの自動電源投入／遮断」
- 255 ページの「電源オプション－サーバの電源制御の設定」
- 258 ページの「電源装置情報－電源装置および FRU 部品の IDPROM データ」

7.6.1 Power ON/OFF －サーバの自動電源投入／遮断

「*Power On/Off*」ページは、管理サーバの電源オン／オフを行います。サーバの現在の電源状態が表示され、そして、次回の起動時のサーバの設定を行うことができます。

図 121：Power ON/OFF ページ

電源状態概要

「電源状態概要」グループは、サーバの現状の電源状態の情報および最も最近のサーバの電源オン／オフの理由を表示します。
それに加えて、サーバの電源が投入されてからの経過時間（年月日分）を表示します。

電源状態概要

電源状態:	Power ON
電源投入からの稼働時間:	3ヶ月 22日 23時間 45分
電源投入要因:	Reboot after warm start
電源切断要因:	Power off - Power Switch

図 122：Power ON/OFF ページ電源状態概要

起動オプション

「起動オプション」グループは、次回起動時のシステム構成を設定することができます。BIOS がシステム起動プロセスを停止している場合、あるいは、POST フェーズでエラーが発生した場合に設定することができます。

ここで設定するオプションは、次回の起動時のみ有効になります。その後、初期設定が再び適用されます。

図 123：電源制御－起動オプションページ

➢「エラー停止設定」リストから、望ましい BIOS の動作を選択してください。

「起動継続」
POST フェーズ中にエラーが発生しても、起動プロセスを継続します。

「エラー時は停止」
POST フェーズ中にエラーが発生した場合、起動プロセスを停止します。

➢「起動デバイス選択」リストから、起動を開始するストレージメディアを選択してください。
次のオプションを選択できます：

- 「*変更なし*」：システムは前回と同じストレージメディアから起動します。
- 「*PXE / iSCSI*」：システムはネットワーク上の PXE あるいは iSCSI から起動します。
- 「*ハードドライブ*」：システムはハードディスクから起動します。
- 「*CDROM / DVD*」：システムは CD あるいは DVD から起動します。
- 「*フロッピー*」：システムはフロッピーディスクから起動します。

➢ *[適用]* ボタンをクリックして、設定を有効にしてください。

電源制御 －サーバの電源投入・切断／サーバの再起動

「電源制御」グループを使って、サーバの電源投入／切断、あるいは、サーバの再起動を行うことができます。

電源制御
電源投入
電源切断
ハードリセット
電源ボタンを押す 2
電源Off-ON
電源切断(シャットダウン) 1
リセット(シャットダウン) 1
適用

図 124：電源投入／切断ページ、再起動（サーバ電源投入）

図 125 ：電源投入／切断ページ、再起動（サーバ電源切断）

「*電源投入*」
サーバの電源を投入します。

「*電源切断*」
オペレーティングシステムの状態にかかわらず、サーバの電源を切断します。

「*ハードリセット*」
オペレーティングシステムの状態にかかわらず、サーバを再起動します（コールドスタート）。

「*電源ボタンを押す*」
インストールされたオペレーティングシステムおよび動作設定により、電源オフボタンを押すことによって、さまざまな動作のトリガーとなります。これらの動作は、コンピュータのシャットダウンや、スタンバイモードあるいはスリープモードへの切り替えである場合があります。

「*電源 OFF-ON*」
サーバの電源を完全に停止して、一定の待機時間の後、再び電源が投入されます。「ASR&R Options (ASR&R オプション)」グループ（286 ページ参照）の「電源サイクル待機時間」フィールドにこの待機時間を設定することができます。

「*電源切断（シャットダウン）*」

適切にシャットダウンし、電源を切断します。
このオプションは、iRMC S2 上に ServerView エージェントがインストールされ、かつ、「接続」と署名されたときにのみ有効です。

「*リセット（ シャットダウン）*」

適切にシャットダウンし、再起動します。
このオプションは、iRMC S2 上に ServerView エージェントがインストールされ、かつ、「接続」と署名されたときにのみ有効です。

➢［*適用*］ボタンをクリックして、設定を有効にしてください。

7.6.2 電源制御オプション－サーバの電源制御の設定

「電源制御オプション」ページを使って、停電後のサーバ動作およびサーバの電源オン／オフ時刻の設定を行うことができます。

図 126 ：電源制御オプションページ

電源復旧時動作設定－停電時サーバ動作の設定

「電源復旧時動作設定」グループを使って、停電時のサーバの電源復旧時動作を設定することができます。

電源復旧時動作設定

○ 電源投入しない
○ 電源投入する
◉ 電源断前の状態に戻す

適用

図 127 ：電源制御オプションページ、電源復旧時動作

「*電源投入しない*」
停電後は、常にサーバは電源オフのままにします。

「*電源投入する*」
停電後は、常にサーバは電源オンにします。

「*電源遮断前の状態に戻す*」
停電前のサーバの電源オン／オフ状態に復旧します。

- 停電前のサーバの電源オン／オフ状態に復旧します。

設定した動作は、停電後に実行されます。

自動電源投入／切断時刻設定－サーバの自動電源投入／切断時刻設定

「自動電源投入／切断時刻設定」入力フィールドグループを使って、特定の曜日あるいは特定の期間のサーバの自動電源投入／切断時刻を設定することができます。

> **i** 「毎日」設定フィールドが最優先です。

「Trap」フィールドを使って、iRMC S2 が予定された管理サーバの電源投入／切断前に SNMP トラップを管理コンソールに送信したりすることができます。そうすることによって、電源投入／切断が何分前に行われるのかを通知することができます。値に「0」を設定すれば、トラップは送信されません。

図 128 ：電源制御オプションページ、自動電源投入／切断時刻

➤［*適用*］ボタンをクリックして、設定を有効にしてください。

7.6.3 電源装置情報 – 電源装置および FRU 部品の IDPROM データ

「電源装置情報」ページは、電源装置およびサーバの FRU の IDPROM データに関する情報を提供します。

「 *CSS* 対象」列は、それぞれの部品が顧客自己保守機能をサポートしているか否かを表しています。

図 129 ：電源装置情報ページ

7.7 電力制御－サーバに設定可能な機能の制御

「*電力制御*」エントリは、管理サーバに設定可能な機能のページのリンクを含んでいます：

– 260 ページの「消費電力制御－サーバに設定可能な機能の設定」

– 255 ページの「電源制御オプション－サーバの電源制御の設定」（iRMC S2 の一部のサーバでは表示されません。）

– 267 ページの「消費電力履歴－サーバの消費電力の表示」（iRMC S2 の一部のサーバでは表示されません。）

7.7.1 消費電力制御 – サーバに設定可能な機能の設定

「*消費電力制御*」ページを使って、iRMC S2 が PRIMERGY サーバの電力制御に使用するモードを設定することができます。

図 130 ：消費電力制御ページ

前提条件：
電力制御を行うには以下の条件を満たす必要があります。
– PRIMERGY 管理サーバが、この特徴をサポートしていなければなりません。
– 「*エンハンススピードステップ*」オプションが BIOS セットアップで有効でなければなりません。

「*電力制御オプション*」グループ、あるいは「電力制御スケジュール」、消費電力モニタリングモードを設定した場合、「電力制御オプション」グループも表示されます（274 ページ参照)。

電力制御のオプション

「*電力制御オプション*」グループを使って、電力制御モードを選択し、消費電力の時間的経過を監視するか否かを設定することができます。

「*電力制御モード*」
管理サーバの消費電力制御モードは以下の通りです。

– 「*電力制御を行わない*」

iRMC S2 は、オペレーティングシステムに電力制御を許可します。

– 「*ベストパフォーマンス*」

iRMC S2 は、サーバがベストパフォーマンスになるよう電力制御を行います。この場合、消費電力量が増える可能性があります。

– 「*最小消費電力*」

iRMC S2 は、最小消費電力を達成するようにサーバを制御します。この場合、サーバのパフォーマンスは常に理想的であるとは言えません。

– 「*電力制限*」

「電力制限オプション」グループが表示されます（276 ページの電力制限オプションを参照）。

– 「*スケジュール*」

iRMC S2 は、SCU (262 ページの「電力制御のスケジュール」を参照) を使って定義したスケジュールにしたがって、電力制御を行います。

「*消費電力監視単位*」
消費電力を表示する単位は以下の通りです：

– 「*Watt*」

– 「 *BTU/h*（BTU ／時（British Thermal Unit ／時、1 BTU ／時は、0.293 ワットに対応します。)」

「*消費電力モニタリング有効*」
　このオプションを有効にした場合、消費電力は連続的に監視されます。

> i 電力監視は、バージョン 3.32 以降のファームウェアバージョンにて初期設定で有効になります。

> i この設定は、電力監視をサポートする PRIMERGY サーバにのみ有効です。

- [*適用*] ボタンをクリックして、設定を有効にしてください。

電力制御スケジュール

「電力制御スケジュール」グループを使って、iRMC S2 が管理サーバの消費電力を制御する詳細なスケジュールおよびモード（オペレーティングシステムによる制御、ベストパフォーマンス、最小電源消費）を設定することができます。

> i 「電力制御スケジュール」グループは、「電力制御オプション」グループの電力制御モードを「スケジュール」に設定した場合にのみ表示されます。

> i 電力制御スケジュールモードの設定には、「エンハンススピードステップ」オプションが BIOS 設定で可能であることが条件です。もしそうでなければ、その旨のメッセージが表示されます。
>
> このメッセージが、「エンハンススピードステップを有効にしてください。」の場合、以下の理由が考えられます。
>
> – サーバの CPU（例えば、能力の低い CPU で）が、電力制御スケジュールをサポートしていない場合があります。
>
> – システムが、BIOS POST フェースである場合があります。

図 131 ：電力制御設定ページ（スケジュール）

「時刻 1」
: iRMC S2 が、「モード 1」で、指定する曜日に電力制御を開始する時刻 [hh : ss]

「時刻 2」
: iRMC S2 が、「モード 2」で、指定する曜日に電力制御を開始する時刻 [hh : ss]

「モード 1」
: iRMC S2 が、「時刻 1」で、指定する曜日に使用するよう設定された電力制御モード

「モード 2」
: iRMC S2 が、「時刻 2」で、指定する曜日に使用するよう設定された電力制御モード

i 「時刻 1」＜「時刻 2」と設定してください。そうしないと「モード 2」のみが、指定した曜日の「時刻 2」に有効になります

i 「毎日」設定フィールドが最優先です。

➢ ［適用］ボタンをクリックして、設定を有効にしてください。

サーバの設定（398 ページの「iRMC 消費電力制御 – サーバ電力制御設定」の章を参照）を使って、電力制御スケジュールを構成することができます。

電力制御オプション

「電力制御オプション」グループは、次の情報を表示します：

– 「電力制御オプション」グループで、選択および有効化された「電力制限」制御モード
– 「電力制御オプション」グループで、「スケジュール」に設定された電力制御モード、および、「 消費電力制御スケジュール」グループのなかで少なくとも一度有効化された「電力制限」電力制御モード

この電力制御モードで有効化された「消費電力制御スケジュール」グループは、すべての期間の電力制限にも適用されます。

図 132：電力制御設定ページ（スケジュール）

「電力制限」
　　最大消費電力（単位：ワット）

「*警告しきい値*」

最大消費電力のパーセンテージでしきい値が、「電力制限」の下に表示されています。しきい値に達すると、「電力制限到達時の動作」の下に定義された動作が実行されます。

「*電力制限の据置期間*」

電力制限のしきい値に到達してから、電力制限到達時の動作が実行されるまでの待機時間（分）を指します。

「*電力制限到達時の動作*」

電力制限に到達し、待機時間が経過したときの動作を指します。

「*継続起動する*」

動作は行われません。

「*電源切断（シャットダウン）*」

システムを「適切に」シャットダウンし、電源を切断します。

このオプションは、iRMC S2 上に ServerView エージェントがインストールされ、かつ、「接続」と署名されたときにのみ有効です。

「*電源切断*」

オペレーティングシステムの状態にかかわらず、緊急にサーバの電源を切断します。

「*動的な電力制御を有効にする*」

電力制限を動的に制御します。

7.7.2 現在のシステム消費電力－現在のシステム消費電力の表示

MC S2 の付属したすべての PRIMERGY サーバでサポートされていません。

「現在のシステム消費電力」ページは、コンポーネントおよびシステムの現在のシステム消費電力を表示します。

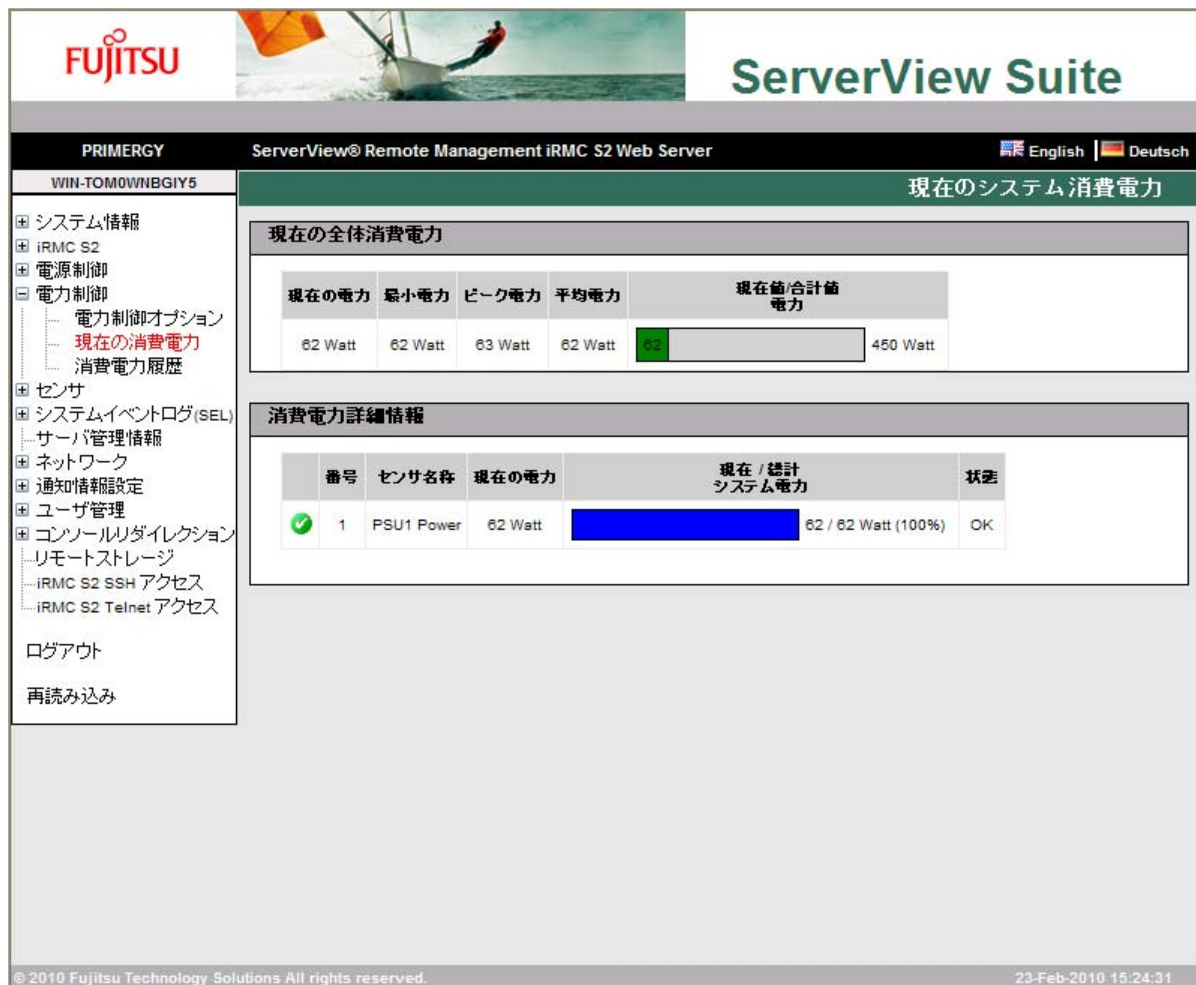



図 133 ：現在のシステム消費電力ページ

7.7.3 消費電力モニタリング履歴 – サーバの消費電力の表示

「消費電力モニタリング履歴」ページは、PRIMERGY サーバの消費電力のグラフを表示します。

> **i** このページは、iRMC S2 の一部の PRIMERGY サーバでサポートされていません。

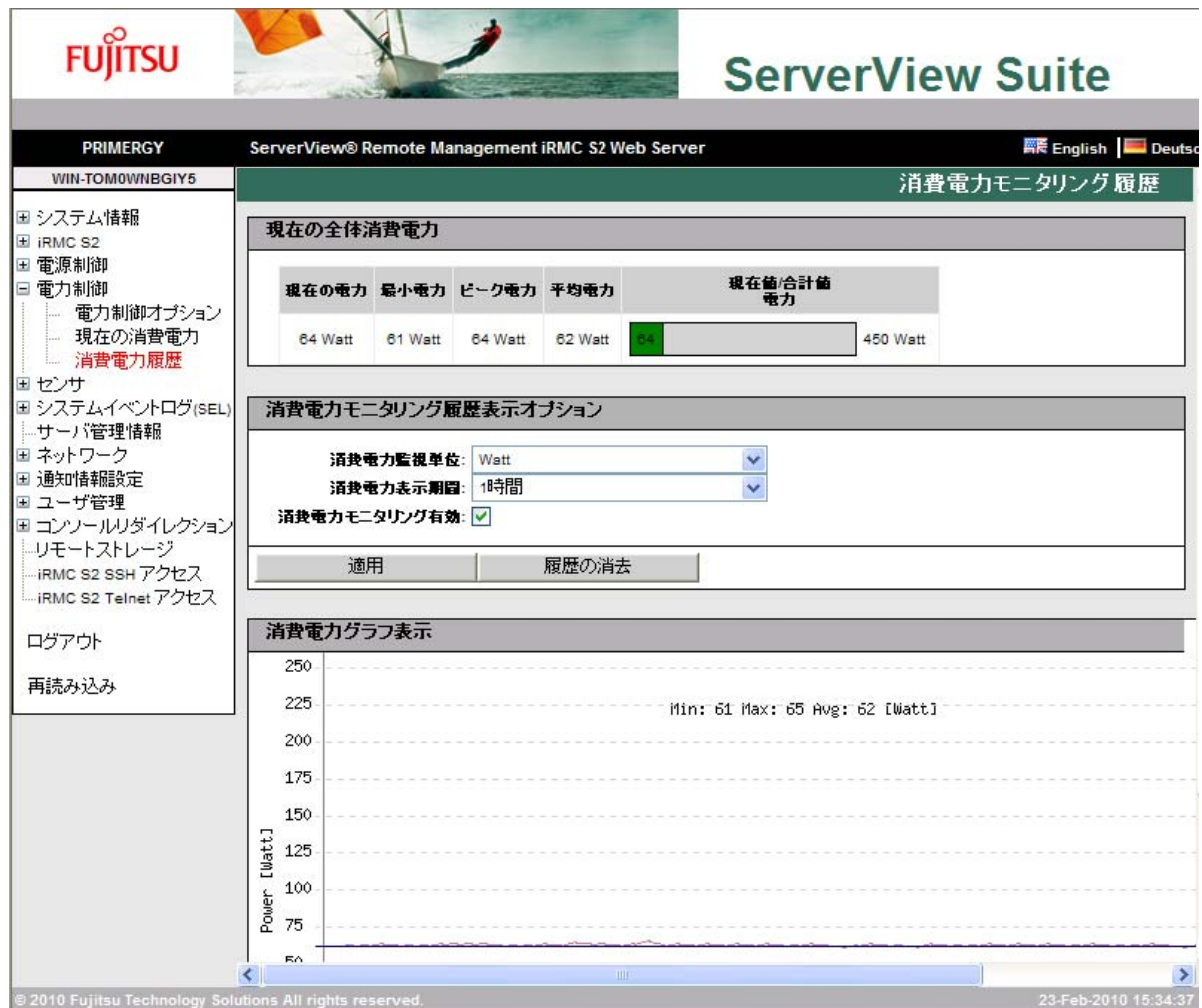



図 134：消費電力モニタリング履歴ページ

現在の全体消費電力

この画面は、一部の PRIMERGY サーバでサポートされていません。

「*現在の全体消費電力*」では、現状設定された間隔で計測したサーバの消費電力の情報が表示されています。現在の電力、最小電力、ピーク電力および平均電力が表示されます。

グラフィカルな表示は、サーバの可能なピーク電力と現在の電力を比較して表示しています。

現在の全体消費電力

現在の電力	最小電力	ピーク電力	平均電力	現在値/合計値 電力
62 Watt	61 Watt	62 Watt	61 Watt	62　450 Watt

図 135：消費電力モニタリング履歴－現在の全体消費電力

消費電力モニタリング履歴表示オプション

消費電力モニタリング履歴表示オプションでは、消費電力を表示するパラメータを設定することができます。

図 136：消費電力モニタリング履歴－消費電力モニタリング履歴表示オプション

「*消費電力監視単位*」

電力単位：

- 「Watt」
- 「 BTU/h （BTU ／時（British Thermal Unit ／時、1 BTU ／時は、0.293 ワットに対応します。）

「*消費電力表示期間*」

消費電力のグラフの表示期間を指します。
以下の間隔が選択可能です：

「*1 時間*」

初期設定です。
最新の 1 時間を計測します（60 の値）。1 分間毎に計測が行われますので、最新の
1 時間の計測値を表示します。

「*12 時間*」

最新の 12 時間を計測します。5 分間隔で計測され、表示されます（5 番毎の計測、
すべてで 144 の値）。

「*1 日*」

最新の 24 時間を計測します。10 分間隔で計測し、表示します（10 番毎の計測、
すべてで 144 の値）。

「*1 週間*」

最新の 1 週間を計測します。1 時間間隔で計測し、表示します（60 番毎の計測、
すべてで 168 の値）。

「*2 週間*」

最新の 1 週間を計測します。およそ 4 時間間隔で計測し、表示します（120 番毎の計測、
すべてで 168 の値）。

「*1 ヶ月*」

最新の 6 ヶ月を計測します。およそ 1 日間隔で計測し、表示します（240 番毎の 計測、
すべてで 180 の値）。

「*1 年*」

最新の 12 ヶ月を計測します。2 日間隔で計測され、表示されます（2880 番毎の 計測、
すべてで 180 の値）

「消費電力モニタリング有効」
電力監視のグラフを表示するか否かを設定します。

電力監視は、バージョン 3.32 以降のファームウェアバージョンでは、初期設定で有効になります。

この設定は、消費電力のロギングをサポートしている PRIMERGY サーバのみに適用できます。

➢ ［*適用*］ボタンをクリックして、設定を有効にしてください。

➢ ［*履歴の消去*］ボタンをクリックして、画面に表示されているデータを消去します。

消費電力グラフ表示

「消費電力グラフ表示」は、グラフ形式で管理サーバの消費電力量を表示します（「消費電力履歴オプション」を利用します)。

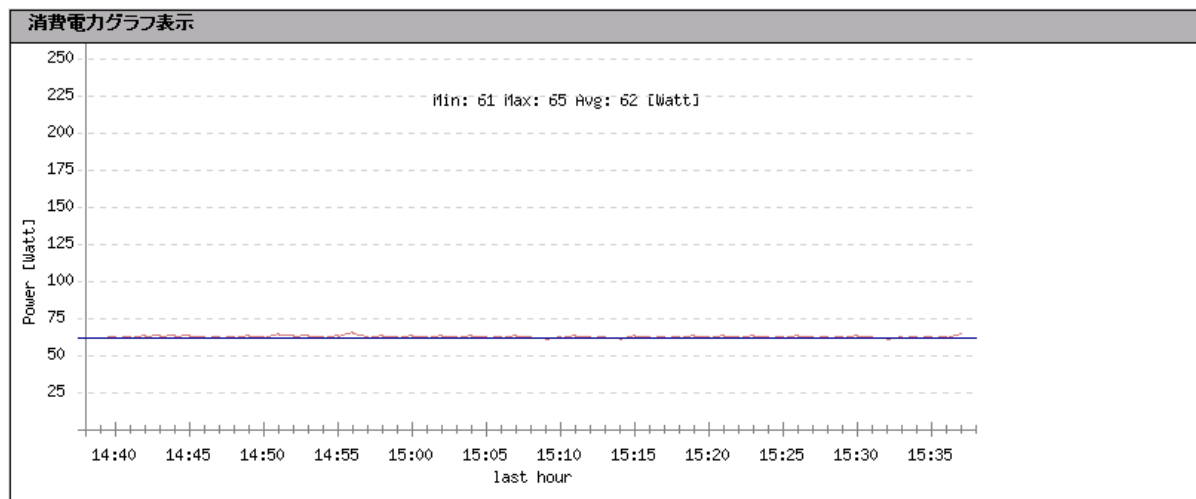



図 137 ：消費電力モニタリング履歴－消費電力グラフ表示オプション

7.8 センサの状態確認

「センサ」エントリは、管理サーバのセンサをテストするページを提供します：

– 272 ページの「ファン－ファンの状態確認」

– 274 ページの「温度－温度センサの状態確認」

– 276 ページの「電圧－電圧センサの状態確認」

– 276 ページの「電圧－電圧センサの状態確認」

– 278 ページの「コンポーネントの状態－サーバのコンポーネントの状態確認」

状況のチェックを容易にするために、センサの状態は、現在値を表示するだけでなく、色コードや状態アイコンも使っています：

黒／	計測値は、通常稼動値範囲です。
オレンジ／	計測値は、警告のしきい値を超えています。 システムの稼動状態は、まだ危険な状態ではありません。
赤／	計測値は、危険のしきい値を超えています。 システムの稼動状態は、危険な状態にある可能性があり、データ喪失の危険があります。

表 7 ：センサの状態

7.8.1 ファン－ファンの状態確認

「ファン」ページは、ファンおよびそれらの状態に関する情報を提供します。

図 138 : ファンページ

ファンテストーファンのテスト

「ファンテスト」グループを使って、ファンのテストを自動的開始する時刻を設定したり、あるいは手動で開始したりすることができます。

「ファンテスト時刻」
　ファンのテストを自動的に開始する時刻を入力してください。
「ファンテストを無効化」
　このオプションを選択すると、ファンのテストが行われなくなります。

➢［適用］ボタンをクリックして、設定を有効にしてください。

➢［ファン回転数テスト開始］ボタンをクリックして、ファンのテストを開始してください。

アナログファンーファンが故障した場合のサーバ動作の設定

「*アナログファン*」グループを使って、ファンの状態に関する情報を確認することができます。オプションおよびボタンを個々のファンあるいはすべてのファンに対して有効にすることができます。また、ファンが故障した場合、何秒後にサーバをシャットダウンすべきか否かを設定することができます。

［*すべて選択*］
　すべてのファンを選択します。

［*すべて選択解除*］
　すべての選択を解除します。

➢ 故障時に特別な処置を行うファンを選択します。

➢ ワークエリアの下方のボタンリストを使って、故障発生時の動作を定義します。

- ［継続稼働］を選択すると、選択されたすべてのファンが故障してもサーバはシャットダウンされません。
- ［シャットダウンと電源切断］を選択すると、選択されたファンが故障した場合、サーバはシャットダウンされ、かつ、電源が切断されます。このオプションを選択する場合、リストの右　のフィールドに、ファンの故障からシャットダウンまでの時間（シャットダウン待機時間）を設定しなければなりません。

i　予備のファンがある場合、「シャットダウンと電源切断」がこれらのファンに設定されると、1 つ以上のファンが故障したときに、シャットダウンが実行されます。

➢［選択したファンに適用］ボタンをクリックして、ファンへの設定を有効にしてください。

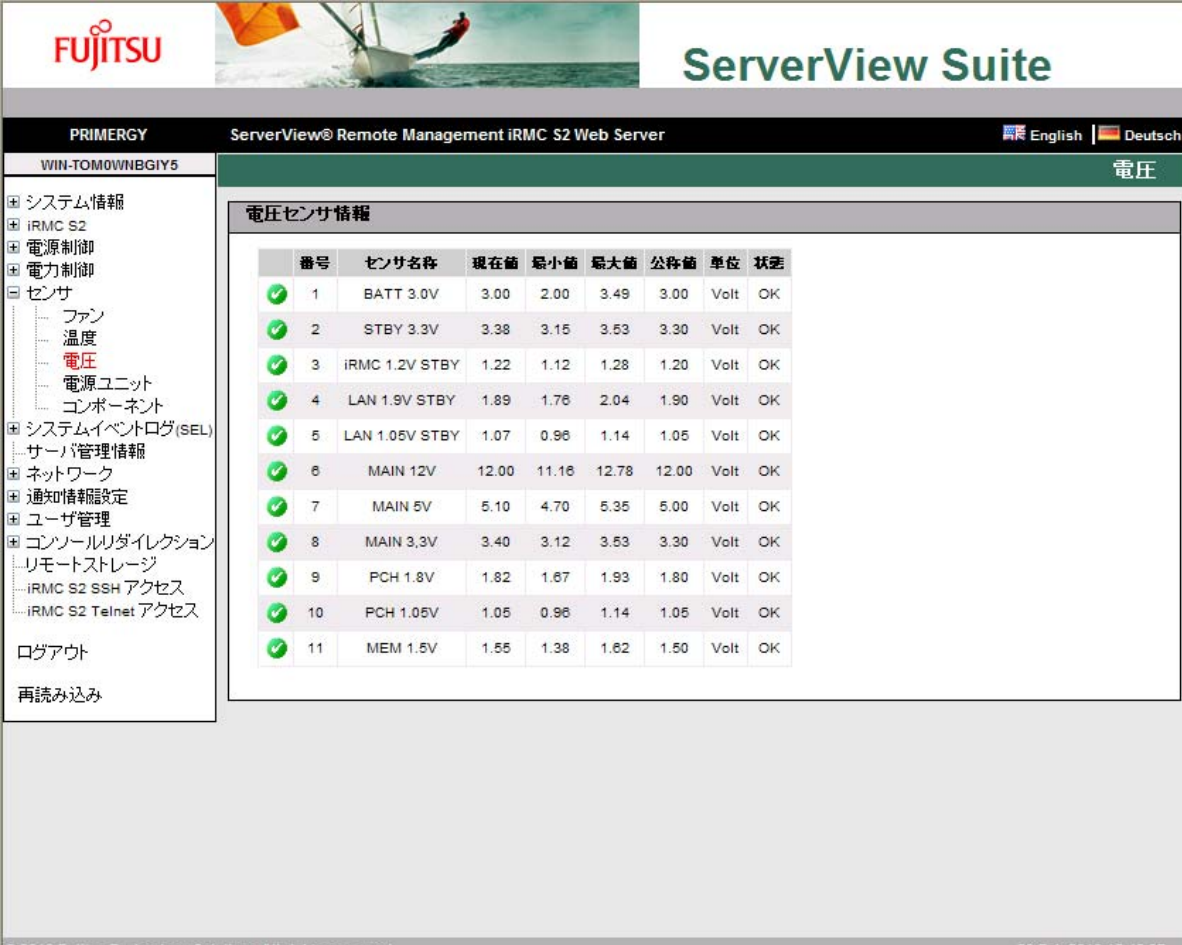
7.8.2 温度 – 温度センサの状態確認

「温度」ページは、たとえば、CPU、FBD（FullyBuffered DIMM）および周囲の温度など、センサが計測したサーバのコンポーネントの温度情報を提供します。

図 139 : 温度ページ

オプションおよびボタンを、個々の温度センサあるいはすべての温度センサに対して有効にすることができます。また、選択されたセンサが危険温度に達した場合、サーバをシャットダウンすべきか否かの設定を行うこともできます。

［*すべて選択*］

すべての温度センサを選択します。

［*すべて選択解除*］
　すべての選択を解除します。

➤ 危険温度に達した場合の動作を定義するセンサを選択してください。

➤ ワークエリアの下方のボタンリストを使って、危険温度到達時の動作を定義します：

– ［継続稼働］を選択すると、選択されたセンサが危険温度に達してもサーバはシャットダウンされません。

– ［継続稼働］を選択すると、選択されたセンサが危険温度に達してもサーバはシャットダウンされません。

➤ ［*選択したセンサに適用*］ボタンをクリックして、温度センサへの設定を有効にしてください。

7.8.3 電圧 – 電圧センサの状態確認

「*電圧*」ページは、サーバのコンポーネントに設定された電圧センサの状態に関する情報を提供します。

	番号	センサ名称	現在値	最小値	最大値	公称値	単位	状態
	1	BATT 3.0V	3.00	2.00	3.49	3.00	Volt	OK
	2	STBY 3.3V	3.38	3.15	3.53	3.30	Volt	OK
	3	iRMC 1.2V STBY	1.22	1.12	1.28	1.20	Volt	OK
	4	LAN 1.9V STBY	1.89	1.76	2.04	1.90	Volt	OK
	5	LAN 1.05V STBY	1.07	0.96	1.14	1.05	Volt	OK
	6	MAIN 12V	12.00	11.16	12.78	12.00	Volt	OK
	7	MAIN 5V	5.10	4.70	5.35	5.00	Volt	OK
	8	MAIN 3,3V	3.40	3.12	3.53	3.30	Volt	OK
	9	PCH 1.8V	1.82	1.67	1.93	1.80	Volt	OK
	10	PCH 1.05V	1.05	0.96	1.14	1.05	Volt	OK
	11	MEM 1.5V	1.55	1.38	1.62	1.50	Volt	OK

図 140 ：電圧ページ

7.8.4 電源装置 – 電源装置の状況確認

「*電源装置個別情報*」ページは、電源装置に関する情報を提供します。

図 141 ：電源装置個別情報

7.8.5 センサの状態 – サーバのコンポーネントの状態確認

「センサの状態」ページは、サーバのコンポーネントの状態に関する情報を提供します。「*CSS* 対象」列は、コンポーネントが、CSS（顧客自己保守）をサポートしているか否かを示しています。

番号	センサ名称	センサ種類ID	センサ種類別通し番号	LED点灯状況	信号状態	CSS対象
1	Ambient	External Environment	0	No	OK	No
2	CPU	Processor	0	No	OK	No
3	DIMM-1A	Memory Device	0	Yes	OK	Yes
4	DIMM-2A	Memory Device	1	Yes	空きスロット	Yes
5	DIMM-3A	Memory Device	2	Yes	空きスロット	Yes
6	DIMM-1B	Memory Device	3	Yes	空きスロット	Yes
7	DIMM-2B	Memory Device	4	Yes	空きスロット	Yes
8	DIMM-3B	Memory Device	5	Yes	空きスロット	Yes
9	FAN1 SYS	Fan/Cooling Device	1	Yes	OK	Yes
10	FAN PSU1	Power Supply	4	No	OK	Yes
11	FAN PSU2	Power Supply	8	No	搭載されていません	Yes
12	BATT 3.0V	Battery	0	No	OK	No
13	Voltages	System Board	0	No	OK	No
14	Temp	External Environment	0	No	OK	No
15	BBU	Battery	1	No	N/A	Yes
16	PSU Connector	Cable/Interconnect	0	No	OK	No
17	PSU1	Power Supply	4	Yes	OK	Yes
18	PSU2	Power Supply	8	Yes	搭載されていません	Yes
19	Power Level	Power Monitoring	1	No	OK	No

図 142：センサの状態ページ

7.9 システムイベントログ（セル）－サーバイベントログの表示および設定

「システムイベントログ」エントリは、サーバイベントログ（システムイベントログ（セル））の表示および設定ページのリンクを含んでいます。

– 280 ページの「システムイベントログの内容－セル上の情報表示およびセル入力」

– 283 ページの「システムイベントログの設定－セルの設定」

色付きのアイコンが、それぞれのイベントあるいはエラーカテゴリに対応しています：

	危機的状況
	重要
	注意
	情報
	顧客自己保守（CSS ）イベント

表 8 ： システムイベントログの内容－エラーカテゴリ

7.9.1 システムイベントログ内容－セル上の情報表示およびセル入力

「システムイベントログ内容」ページは、セル上の情報およびセル入力の表示を提供します。「*CSS* 対象」列は、イベントが、CSS （顧客自己保守）をトリガーにしているか否かを示しています。

図 143 ：システムイベントログ内容ページ

システムイベントログ（SEL）情報

「*システムイベントログ（SEL）情報*」グループは、セル内のエントリ番号の情報を提供します。それは、また、最新のエントリが加えられたり、削除された時刻を示します。

システムイベントログ(SEL)情報

イベントログの状態: 425 Entries of 425 (Ring SEL)
最新のエントリ: 23-Feb-2010 15:53:07
クリア日時: 16-Dec-2009 14:55:03

ログのクリア　ログの保存

図 144 ：システムイベントログの内容ページ、システムイベントログ（SEL）情報

［*ログのクリア*］
　［ログのクリア］ボタンをクリックすると､セル内のすべてのエントリを消去することが できます。

［*ログの保存*］
　［ログの保存］ボタンをクリックした後、iRMC S2 が、セルのエントリを含んだ iRMC *S2_EventLog.sel* ファイルのダウンロードを許可します。

システムイベントログ内容

「システムイベントログ内容」グループは、エラークラスによってフィルタリングされたエントリを表示します。

「*システムイベントログ内容*」グループの動作中に、フィルタリングの設定を変更することができます。この設定は、ログアウト後有効になります。

	発生日時	重要度	発生元	内容	種別	CSS対象
	23-Feb-2010 15:55:30	情報(Info)	Microsoft	Operating system boot 23-Feb-2010 15:55:25	System Status	No
	23-Feb-2010 15:55:30	情報(Info)	SMS	Boot from hard drive completed	System Status	No
	23-Feb-2010 15:53:07	情報(Info)	iRMC S2	Powered on by a PCI bus power management event	System Power	No
	23-Feb-2010 15:24:30	情報(Info)	Power Level	System power consumption within limit	System Power	No
	23-Feb-2010 15:24:22	情報(Info)	Power Level	System power consumption limiting disabled	System Power	No
	23-Feb-2010 15:22:15	情報(Info)	Power Level	System power consumption within limit	System Power	No
	23-Feb-2010 15:19:20	情報(Info)	Power Level	System power consumption limiting disabled	System Power	No
	23-Feb-2010 14:54:33	情報(Info)	iRMC S2	iRMC S2 Browser user 'admin' login from 10.21.136.105	Security	No
	23-Feb-2010 14:33:10	情報(Info)	iRMC S2	iRMC S2 Browser user 'admin' login from 10.21.136.105	Security	No
	23-Feb-2010 13:59:07	情報(Info)	iRMC S2	iRMC S2 Browser user 'admin' login from 10.21.136.105	Security	No

図 145 ：システムイベントログの内容ページ、システムイベントログの内容

「*危険(Critical)を表示*」、「*重要(Major)を表示*」、「*軽度(Minor)を表示*」、「*情報(Info)を表示*」、「*CSS 対象のみ表示*」

一つのみのレベル選択、あるいは、複数のレベル選択を行うことができます。

➢ ［*適用*］ボタンをクリックして、現状セッションの間に設定を有効にしてください。

7.9.2 システムイベントログ設定－セルの設定

「*システムイベントログ設定*」ページで、以下の設定が可能です。

– セルには、「システムイベントログ内容」ページ（280 ページ参照）記載の情報が表示されます。

– セルは、リングバッファあるいはリニアバッファとして構成されています。

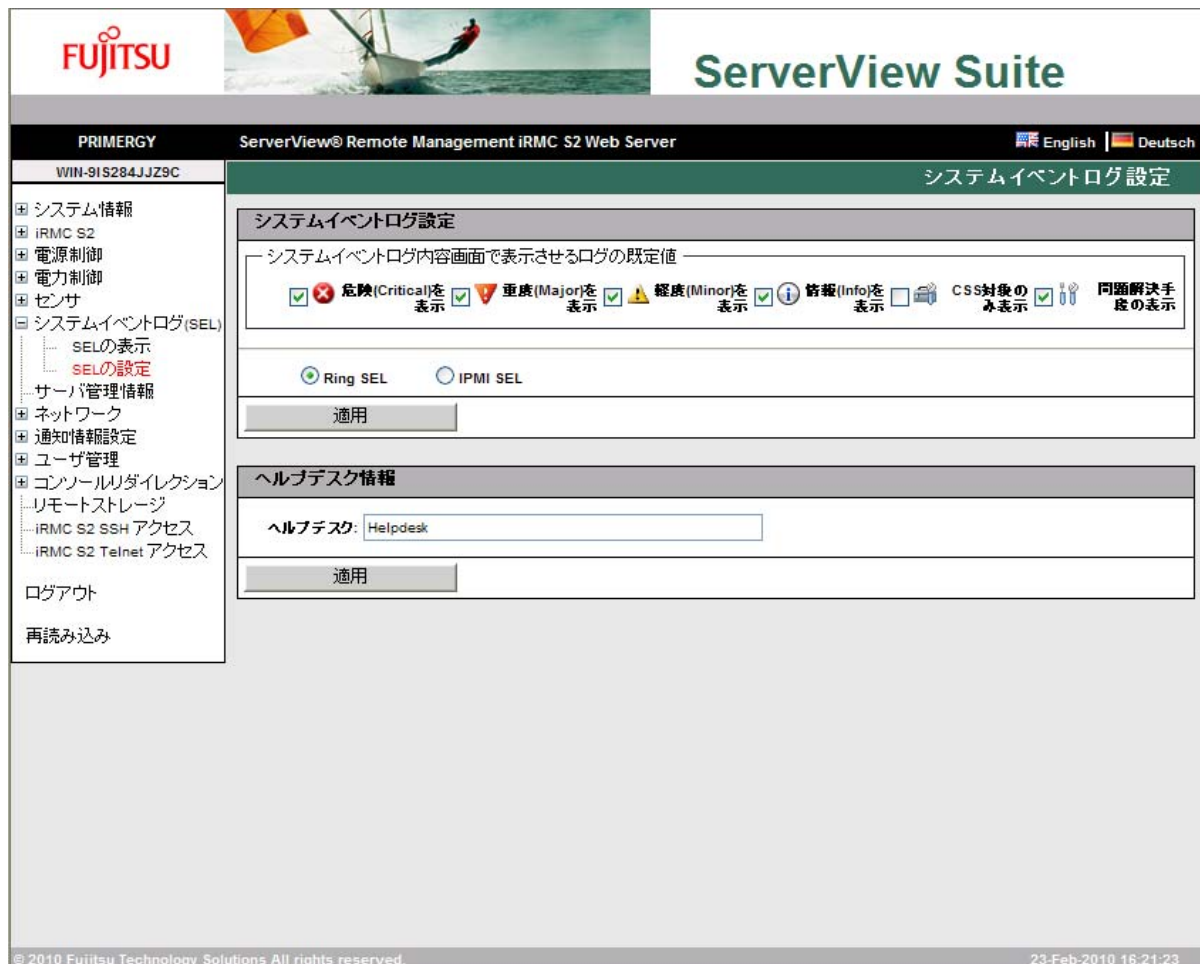



図 146：システムイベントログ設定ページ

システムイベントログ内容

「システムイベントログ内容」グループの動作中に、フィルタリングの設定を変更することができます。
この設定は、ログアウト後有効になります。

「危険（Critical）を表示」、「重要（Major）を表示」、「軽度（Minor）を表示」、「情報（Info）を表示」、
「CSS 対象のみ表示」

「システムイベントログ内容」ページを使って、セルに表示される一つあるいは複数のレベルを選択することができます。

管理 PRIMERGY サーバに、ServerView ローカルサービス表示モジュール が利用できる場合は、セルに表示するエラーを ServerView ローカルサー ビス表示モジュールパネルからも選択することができます。（ここでの選択は、「システムイベントログ内容」ページで設定した内容と独立したものになります。）

［**Ring SEL**］
セルは、リングバッファとして構成されます。

［**IPMI SEL**］
セルは、リニアバッファとして構成されます。

リニアセルが完全に一杯となった場合は、それ以上のエントリを追加できなくなります。

➢［適用］ボタンをクリックして、設定を有効にしてください。

ヘルプデスク情報

ヘルプデスク情報
ヘルプデスク: Helpdesk
適用

図 147：ヘルプデスク情報

「*ヘルプデスク*」
ヘルプデスクが表示されます

➢［*適用*］ボタンをクリックして、設定を有効にしてください。

7.10 サーバ管理情報－サーバ設定

「サーバ管理情報」ページを使って、サーバ上の以下の構成を行うことができます：

– サーバの ASR&R 設定（286 ページ参照）

– ウォッチドッグ設定（287 ページ参照）

– HP System Insight Manager (HP SIM) との連携（288 ページ参照）

図 148 ：サーバ管理情報ページ

ASR&R オプション－ ASR&R 設定

「ASR&R オプション」グループを使って、サーバの ASR&R 設定を行うことができます。

> i 「ASR&R オプション」グループで行う設定は、管理サーバの次回の起動時から有効になります。

ASR&Rオプション

ASR&R起動間隔(1 - 30): 2 分
リトライ カウンタ 最大値(0 - 7): 1
リトライ カウンタ(0 - Max): 1
BIOSの自動書換: 無効
パワー サイクル間隔(0 - 15): 5 秒
適用

図 149：サーバ管理情報ページ、ASR&R オプション

「*リトライカウンタ最大値（0 - 7）*」
: サーバの危機的エラー発生後の最大リスタート許可回数（最大 7 回）を指します。

「*リトライカウンタ（0 - Max）*」
: サーバの危機的エラー発生後の（「リトライカウンタ最大値」に設定された値以下）リスタート回数を表します。

「*BIOS 自動書換*」
: BIOS リカバリフラッシュの有効／無効を設定するビットです：
  - 「有効」
    次回のシステム起動時に、BIOS を自動で書き換えします。
  - 「無効」
    次回のシステム起動時に、BIOS を自動で書き換えしません。

> i この値を「有効」に設定すると、ファームウェアが更新されるまで、オペレーティングシステムは起動しません。BIOS リカバリフラッシュが、次回のシステム起動時に MS-DOS フロッピーから（あるいは MS-DOS フロッピーイメージから）自動で実行されます。
>
> BIOS リカバリフラッシュが成功してから、BIOS リカバリフラッシュビットを「無効」に再設定してください。

「*パワーサイクル間隔（0 - 15）*」
電源オフから電源オンまでの間の間隔（秒）を設定します。

➢ ［適用］ボタンをクリックして、設定を有効にしてください。

設定が保存され、適切な条件がそろうと動作が実行されます。

ウォッチドッグ設定 － ソフトウェアウォッチドッグおよび **Boot** ウォッチドッグの設定

「ウォッチドッグ設定」グループをつかって、ソフトウェアウォッチドッグおよび Boot ウォッチドッグの構成を行うことができます。

「ウォッチドッグ設定」グループで行う設定は、管理サーバの次回の起動時から有効になります。

ウォッチドッグ設定
有効
ソフトウェア ウォッチドッグ: 継続稼働 タイムアウト時間 (1 - 100): 5 分
Bootウォッチドッグ: 継続稼働 タイムアウト時間 (1 - 100): 100 分
適用

図 150 ：サーバ管理情報ページ、ウォッチドッグオプション

ソフトウェアウォッチドッグは ServerView エージェントを使用して、システムの稼働状況を監視します。ソフトウェアウォッチドッグは、ServerView エージェントおよびオペレーティングシステムが完全に初期化されたときに有効になります。

ServerView エージェントは、iRMC S2 に定義された間隔で接触します。ServerView エージェントからのメッセージがない場合、システムは機能的に正しく動作していないと考えられます。このような場合に備えて、実行される動作を設定することができます。

Boot ウォッチドッグは、システムの起動から ServerView エージェントが正常動作するまでのフェーズを監視します。
ServerView エージェントが、サーバの iRMC S2 と一定時間接続を構築できない場合、起動プロセスが正常に行われていないと考えられます。このような場合に備えて、実行される動作を設定することができます。

次の手順で行ってください：

➢ 「ソフトウェアウォッチドッグ」および「Boot ウォッチドッグ」の下のオプションをチェックしたり、チェックを外したりしてください。

➢ これらのオプションを有効にした後、「ソフトウェアウォッチドッグ」および「Boot ウォッチドッグ」の以下の設定を行うことができます。

「*継続稼働*」
ウォッチドッグが時間切れしても、何の動作も行われません、すなわち、サーバは稼動を続けます。イベントログに記録されます。

「*リセット*」
サーバ管理ソフトウェアが、システムリセットを行います。

「*パワーサイクル*」
サーバの電源が遮断され、直ちに、電源投入されます。

➢「タイムアウト時間」の後に、動作が実行されるまでの待機時間（分）を入力してください。

Boot ウォッチドッグは、システムが起動するまで待機します。それゆえ、「タイムアウト時間（0 - 100）」には、十分な時間を設定しなければなりません。

➢［適用］ボタンをクリックしてください。

設定が保存され、適切な条件がそろうと動作が実行されます。

HP System Insight Manager （HP SIM) 連携オプションー HP SIM 連携設定

「HP System Insight Manager（HP SIM) 連携オプション」グループを使って、iRMC S2 デバイスが、HP System Insight Manager から送信される非公式の XML 問い合わせに対する応答として、ある識別情報を返すように設定することができます。

HP SystemInsightManager (HP SIM)連携オプション

SIM連携無効: ☐

適用

図 151 ：サーバ管理情報ページー HP System Insight Manager （HP SIM) 連携オプション

次の手順で行ってください：

➢ HP SIM との連携を無効あるいは有効にするために、「*SIM* 連携無効」オプションを設定してください。

➢［*適用*］ボタンをクリックして設定を有効にしてください。

7.11 ネットワーク設定－ LAN パラメータの設定

「ネットワーク設定」エントリは、iRMC S2 の LAN パラメータを設定するページのリンクを提供します。

– 290 ページの「ネットワークインターフェース iRMC S2 に関するイーサネット設定」

– 293 ページの「ポート番号とネットワークサービス－ポート番号とネットワークサービスの設定」

– 297 ページの「 DHCP 設定－ iRMC S2 のホスト名の設定」

– 297 ページの「 DHCP 設定－ iRMC S2 のホスト名の設定」

7.11.1 ネットワークインターフェース iRMC S2 に関するイーサネット設定

「ネットワークインターフェース」ページを使って、iRMC S2 のイーサネット設定の表示および変更を行うことができます。

図 152：ネットワークインターフェースページ

注意！
イーサネット設定を変更する前に、システムのネットワーク管理責任者に連絡してください。

iRMC S2 のイーサネット設定を誤ると、iRMC S2 にアクセスするには、シリアルインターフェースあるいは BIOS などを使った特殊なソフトウェア構成を使わなければなりません。

「iRMC S2 設定」許可を持つユーザーのみが、イーサネット設定を編集することができます (53 ページの「 iRMC S2 によるユーザー管理」の章を参照)。

「*MAC アドレス*」

iRMC S2 の MAC アドレスがここに表示されます。

「*LAN 接続速度*」

LAN 接続速度を設定します。次のオプションから選択できます。

– 自動検出
– 100 M ビット ／秒 全二重
– 100 M ビット ／秒 半二重
– 10 M ビット ／秒 全二重
– 10 M ビット ／秒 半二重

「自動検出」が選択されると、iRMC S2 のオンボードの LAN コントローラが、自動的に正しい伝送速度および全二重あるいは半二重方式の接続方法を決定します。

「*LAN ポート*」

このオプションは、すべての PRIMERGY サーバでサポートされていません。

ある PRIMERGY サーバモデルでは、NIC (network interface card) システムにインストールされた LAN インターフェースは、以下のいずれかとして設定されます。

– 操作を共有するための共有 LAN システム

あるいは

– LAN 管理を排他的に利用した LAN サービス

「*IP* アドレス」

LAN 内の iRMC S2 の IP アドレスを指します。この IP アドレスは、管理サーバの IP アドレスとは異なります。

「DHCP 有効」オプションが有効になっていない静的な IP アドレス方式で運用している場合、ここに IP アドレスを入力することができます。そうでない場合、つまり、「DHCP 有効」オプションが有効になっている iRMC S2 は、IP アドレスを表示するためだけにこのフィールドを使用します。

「*サブネットマスク*」

LAN 内の iRMC S2 のサブネットマスクを指します。

「*ゲートウェイ*」

LAN 内のデフォルトゲートウェイの IP アドレスを指します。

「*DHCP 有効*」

このオプションを有効にすると、iRMC S2 は、ネットワーク上の DHCP サーバから LAN 設定を取得します。

ネットワーク上に DHCP サーバが存在しない場合は、DHCP オプションを有効にしないでください。
DHCP オプションを有効にし、かつ、ネットワーク上に DHCP サーバが 存在しないと、iRMC S2 は探索ループに入ります (すなわち、DHCP サーバが見つかるまで、探し続けます)。
設定された iRMC S2 は、適切に設定された DHCP サーバ（297 ページの 「DHCP 設定 – iRMC S2 のホスト名の設定」および 299 ページの「 DNS 設定 – iRMC S2 の DNS 使用の有効化」を参照）によって、DNS サーバ に登録することができます。

「*VLAN 有効*」

このオプションは、iRMC S2 の VLAN サポートを有効にします。

「*VLAN ID*」

iRMC S2 が所属する仮想ネットワーク（VLAN ）の VLAN ID を指します。許可される値の範囲：
1 ≦「 VLAN ID」≦ 4094

「*VLAN プライオリティ*」

iRMC S2 の VLAN 優先度（ユーザー優先度）は、VLAN ID によって設定されます。許可される値の範囲： 0 ≦「VLAN プライオリティ」≦ 7 （初期値： 0 ）

➤ ［*適用*］ボタンをクリックして、イーサネット設定を有効にしてください。

7.11.2 ポート番号とネットワークサービス – ポート番号とネットワークサービ スの設定

「ポート番号とネットワークサービスの設定」ページを使って、ポート番号およびネットワークサービスの表示および設定を行うことができます。

図 153 ：ポート番号およびネットワークサービスページ

iRMC S2 Web インターフェースが有効になっていない場合、ポート番号の設定はサポートされません。

Web ベースアクセスのポート

「*セッションタイムアウト*」

通信していない期間（秒）が設定値を経過すると自動的にセッションが閉じられます。iRMC S2 Web インターフェースのログインページが表示され、再びログインするように求められます（210 ページ参照）。

「セッションタイムアウト」より短いリフレッシュ間隔を「自動リフレッシュ間隔」フィールド（295 ページ参照）に入力した場合、「セッションタ イムアウト」に設定された時間が経過しても、自動的にセッションが閉じられません。

「*HTTP* ポート」

iRMC S2 の HTTP ポートを指します。
初期ポート番号： 80
変更可能： はい
初期値の利用： はい
通信方向：inbound & outbound

「*HTTPS ポート*」

i RMC S2 の HTTPS （セキュアな HTTP ）ポートを指します。
初期ポート番号： 443
変更可能： はい
初期値の利用： はい
通信方向： inbound & outbound

「*HTTPS* 接続のみ有効」

「HTTPS 接続のみ有効」オプションを有効にした場合、ユーザーは、iRMC S2 とのセキュアな通信をエントリフィールドに表示された HTTPS ポートで構築することができます。

「HTTPS 接続のみ有効」オプションを無効にした場合、ユーザーは、iRMC S2 とのセキュアでない通信をエントリフィールドに表示された HTTP ポートで構築することができます。

SSL 認証が期限切れした場合、その旨のメッセージがブラウザに表示されます。

「*自動リフレッシュ有効*」

このオプションを有効にすると、iRMC S2 Web インターフェースの画面は、自動的に周期的に再読み込みされます。「自動リフレッシュ間隔」フィールドに、再読み込みの間隔を設定してください。

「*自動リフレッシュ間隔*」

iRMC S2 Web インターフェースが、自動的に再読み込みする間隔（秒）を設定します。

再読み込み間隔の値に「セッションタイムアウト」（294 ページ参照）よりも短い時間を設定した場合、セッションは、「セッションタイムアウト」を経過しても、自動的に閉じられません。

Telnet/SSH アクセス

「*TELNET ポート*」

iRMC S2 の TELNET ポートを指します。
初期ポート番号：3172
変更可能：はい
初期値の利用：いいえ
通信方向：inbound & outbound

「*Telnet ドロップアウト時間*」

通信が行われない期間（秒）が設定値を経過した場合、TELNET 接続は自動的に切断されます。

「*SSH ポート*」

iRMC S2 の SSH （セキュアなシェル）ポートを指します。
初期ポート番号： 22
変更可能：はい
初期値の利用：はい
通信方向：inbound & outbound

「*Telnet 有効*」

「Telnet 有効」オプションを有効にした場合、ユーザーは、エントリフィールドに示された TELNET ポートで、iRMC S2 と接続を構築することができます。

VNC ポート

「*標準ポート*」

セキュアな iRMC S2 の VNC ポートおよびセキュアでないビデオリダイレクションを指します。
ビデオリダイレクション（AVR ）
ポート番号：80
ハードー構成
初期値の利用：はい
通信方向：inbound のみ

「*セキュアポート（SSL）*」

iRMC S2 の VNC ポートは、ビデオリダイレクション入力のマウスおよびキーボード入力を SSL を使って安全に送信します。
ポート番号： 443
ハードー構成
初期値の利用：はい
通信方向：inbound のみ

リモートストレージポート

「*標準ポート*」

iRMC S2 の リモートストレージポートの初期値を指します。
初期ポート番号： 5901
変更可能：はい
初期値の利用：はい
通信方向： リモート管理端末への outbound

➢「*適用*」ボタンをクリックして、設定を保存してください。

7.11.3 DHCP 設定 – iRMC S2 のホスト名の設定

「*DHCP* 設定」ページを使って、以下のように、ダイナミック DNS を利用して、iRMC S2 のホスト名を構成することができます。ダイナミック DNS は、DHCP サーバに識別を容易にするためにネットワーク構成情報として、IP アドレスとシステム名を DNS サーバに自動的に送信します。

図 154：DHCP 設定ページ

「*DHCP アドレスを DNS に登録*」

iRMC S2 の DHCP 名の DNS サーバへの送信を有効／無効にします。

「*ホスト名に、iRMC S2 を使用する*」

「iRMC S2 名」エントリフィールドに入力された iRMC S2 名をサーバ名の代わりに使用します。

「*シリアル番号を付加する*」

iRMC S2 の MAC アドレスの下 3 バイトを iRMC S2 の DHCP 名に追加します。

「*文字列を付加する*」
「文字列」エントリフィールドに設定された内容が 、iRMC S2 の DHCP 名に追加されます。

「*文字列*」
iRMC S2 の拡張名を入力します。

「*iRMC S2 名*」
iRMC S2 名が、サーバ名の代わりに、DHCP に渡されます。

「*DNS 名*」
iRMC S2 の構成された DNS 名を表示します。

7.11.4 DNS 構成－ iRMC S2 の DNS 使用の有効化

「*DNS* 構成」ページを使って、iRMC S2 のドメインネームサービス（DNS）を有効にすることができます。これにより、設定中の iRMC S2 に IP アドレスの代わりに、DNS 名を使うことができます。

図 155：DNS 構成ページ

「*DNS 有効*」

iRMC S2 の DNS を有効／無効に設定します。

「*DHCP から DNS 構成を取得する*」

このオプションを有効にすると、DHCP サーバから、DNS サーバに自動的に IP アドレスが提供されます。

この設定は、最大 5 つの DNS サーバをサポートします。
この設定を有効にしていない場合、5 つの DNS サーバ（「 DNS-Server 1 （DNS サーバ 1)」から「DNS サーバ 5」に手動で、アドレスを入力する必要があります。

「*DNS ドメイン*」

「DHCP から DNS 構成を取得する」オプションが有効になっていない場合、DNS サーバのデフォルトドメインを設定するように要求されます。

「*DNS サーバ 1 - 5*」

「DHCP から DNS 構成を取得する」オプションが有効になっていない場合、ここで、最大 5 つの DNS サーバ名を入力しなければなりません。

➢［*適用*］ボタンをクリックして、設定を保存してください。

7.12 警告通知－警告通知の設定

「警告通知」エントリは、iRMC の警告通知の設定を行う際に利用するページのリンクを含んでいます。

– 302 ページの「 SNMP トラップ通知－ SNMP トラップ通知の設定」

– 303 ページの「シリアル／モデムによる通知－モデムを通した通知の設定」

– 305 ページの「 E-mail による通知－ E-mail による通知の設定」

7.12.1 SNMP トラップ送信設定－ SNMP トラップ通知の設定

「*SNMP* トラップ送信設定」ページを使って、SNMP トラップ通知の設定の表示および構成を行うことができます。

SNMP トラップを最大 *7* つの **SNMP** サーバに送信する機能をサポートしています。

図 **156**：**SNMP** トラップ送信設定ページ

「*SNMP* コミュニティ」

SNMP コミュニティ名を指します。

➢［適用］ボタンをクリックして、コミュニティ名を受け入れてください。

「*SNMP* サーバ *1 - 7*（トラップ送信先）」

コミュニティに所属するサーバの DNS 名あるいは IP アドレスを入力して、「トラップ送信先」を構成してください。

➢ 適用］ボタンをクリックして、トラップの送信先として SNMP サーバを有効にしてください。

➢ テスト］ボタンをクリックして、SNMP サーバとの接続をテストしてください。

➢［すべて適用］ボタンをクリックすると、設定が適切であった場合、すべての設定が有効になります。

7.12.2 シリアル／モデム通知設定－モデム経由通知設定

「シリアル／モデム通知設定」ページを使って、モデムを通した通知の送信方法を設定することができます。本設定は未サポートです。

図 157：シリアル／モデム通知設定ページ

「モデム経由の通知を有効

シリアル／モデム経由の通知を有効あるいは無効に設定します。

「モデム初期化文字列」

ここへの入力に関する詳細は、使用するモデムのユーザーガイドを参照してください。

「モデムリセット／ハングアップ文字列」

ここへの入力に関する詳細は、使用するモデムのユーザーガイドを参照してください。

「モデムプレフィックス番号」

ここへの入力については、使用する接続方式に依存します。

「プロバイダ電話番号」

SMS サーバ名を入力してください。

「ポケットベル電話番号」
ポケットベルの電話番号を入力してください。

「ポケットベルタイプ」
以下の中から選択してください：

– Signal Pager
– Numeric Pager
– Alpha pager
– SMS
– DoCoMo

「SMS メッセージ限度長」
最大値として、80 あるいは 140 文字を選択してください。

「 SMS プロトコルタイプ」
携帯電話が使うネットワークに対応したオプションを選択してください。

➢［適用］ボタンをクリックして、設定を有効にしてください。

➢［テスト］ボタンをクリックして、テストの警告通知を送信してください。

7.12.3 E-mail 設定－ E-mail による通知の設定

「*E-mail* 設定」のページを使って、電子メール通知の設定の構成を行うことができます。

二つのメールサーバに対する構成が行えるようにサポートしています。

E-mail による通知は個々のユーザーに対して設定することができます (314 ページ「ユー ザー‘ユーザー名’ 設定－ユーザー設定（詳細）」の節参照)。

E-mail による通知は、iRMC S2 のディレクトリサービスでのユーザー ID（53 ページ「iRMC S2 によるユーザー管理」の章参照）には、現状、設定できるようにサポートされていません。

図 158：E-mail 設定

E-mail 送信設定－電子メールの設定

「*E-mail* 送信設定」グループを使って、電子メールの設定を行うことができます。

E-mail送信設定

E-mailでの警告送信を有効にする:

SMTPリトライ回数(0 - 7): 3

SMTPリトライ間隔(0 - 255): 30 秒

SMTP応答待ち時間: 45 秒

適用

図 159：E-mail 設定、E-mail 送信設定

「*E-mail 送での警告送信を有効にする*」
　　このオプションを有効にしてください。

「*SMTP リトライ回数（0 - 7 ）*」
　　SMTP のリトライ回数を入力してください。

「*SMTP* リトライ間隔（*0 - 255* ）
　　SMTP リトライ間隔（秒）を設定してください。

「*SMTP* 応答待ち時間」
　　SMTP 応答待ち時間（秒）を設定してください。

➢［適用］ボタンをクリックして、設定を有効にしてください。

プライマリ **SMTP** サーバ設定－プライマリメールサーバ設定

「プライマリ *SMTP* サーバ設定」グループを使って、プライマリサーバ（SMTP サーバ）の設定を行うことができます。

プライマリSMTPサーバ設定

SMTPサーバ: 0.0.0.0

SMTPポート: 25

認証タイプ: 認証を行わない

適用

図 160：E-mail 設定、プライマリ SMTP サーバ設定

「SMTP サーバ」

プライマリメールサーバの IP アドレスを入力してください。

iRMC S2 のドメインネームシステム（DNS）（299 ページの「DNS 設定－ iRMC S2 の DNS 使用の有効化」参照）を有効にすることができます。その場合は、IP アドレスのかわりに、DNS 名を使うことができます。

.

「SMTP ポート」

メールサーバの SMTP ポート番号を入力してください。

「認証タイプ」

iRMC S2 をメールサーバに接続する際の認証方式を選択してください：

– 「認証を行わない

接続時に認証方式は使われません。

– 「*SMTP* 認証（*RFC 2544*）」

RFC 2554 に準拠した認証方式： SMTP サーバの認証方式の拡張です。

この場合、次の情報が必要になります：

「認証ユーザー名」

メールサーバ上で認証されるユーザー名を入力してください。

「認証パスワード」

メールサーバ上で認証されるパスワードを入力してください。

「パスワード確認」

確認用にパスワードを再度入力してください。

➢ ［適用］ボタンをクリックして、設定を有効にしてください。

セカンダリ SMTP サーバ設定－セカンダリメールサーバ設定

「セカンダリ *SMTP* サーバ設定」グループを使って、セカンダリサーバ（SMTP サーバ）の設定を行うことができます。

セカンダリ SMTPサーバ設定

SMTPサーバ: 0.0.0.0
SMTPポート: 25
認証タイプ: 認証を行わない

適用

図 161 : E-mail 設定、セカンダリ SMTP サーバ設定

「*SMTP* サーバ」
セカンダリメールサーバの IP アドレスを入力してください。

> iRMC S2 のドメインネームシステム（DNS）（299 ページの「DNS 設定－ iRMC S2 の DNS 使用の有効化」参照）を有効にすることができます。その場合は、IP アドレスのかわりに、DNS 名を使うことができます。

「*SMTP* ポート」
メールサーバの SMTP ポート番号を入力してください。

「*認証方式*」
iRMC S2 をメールサーバに接続する際の認証方式を選択してください :

– 「認証を行わない」
接続時に認証方式は使われません。

– 「SMTP 認証（RFC 2544 ）」
RFC 2554 に準拠した認証方式 : SMTP サーバの認証方式の拡張です。

この場合、次の情報が必要になります :

「*認証ユーザー名*」
メールサーバ上で認証されるユーザー名を入力してください。

「*認証パスワード*」
メールサーバ上で認証されるパスワードを入力してください。

「パスワードの確認」
確認用にパスワードを再度入力してください。

➤ ［*適用*］ボタンをクリックして、設定を有効にしてください。

E-mail 送信フォーマット－ E-mail 送信フォーマット

「*E-mail* フォーマットの設定」グループを使って、E-mail フォーマット設定を行うことができます。個々のユーザーについて、「*新規ユーザーの設定－ユーザー' ユーザー名 ' 設定－ E-mail 送信フォーマット*」を使って、E-mail フォーマットを設定することができます（318 ページ参照）。

次の **E-mail** フォーマットがサポートされています：

– 「標準メール」
– 「題名固定」
– 「ITS フォーマット」（未サポート）
– 「FujitsuREMCS フォーマット」

図 162：E-mail 設定ページ、E-mail 送信フォーマット

E-mail フォーマットによっては、いくつかの項目が入力できない場合があります。

「*送信元*」
iRMC S2 送信者を識別する情報です。
すべての E-mail フォーマットで入力可能です。

ここに入力された文字列が、「 @ 」を含んでいる場合、その文字列は有効な電子メールアドレスであると解釈されます。 一方で、「 admin@< IP アドレス >」も有効な電子メールアドレスとして使用されます。

「*題名*」
電子メール通知の場合、固定されます。
E-mail フォーマットとして、「題名固定」（318 ページ参照）が有効な場合にのみ、入力可能になります。

「メッセージ」
電子メールのメッセージを入力してください。
E-mail フォーマットとして、「題名固定」（318 ページ参照）が有効な場合にのみ、入力可能になります。

「*管理者名*」

管理責任者の名前を入力します（任意）。
E-mail フォーマットとして、「ITS フォーマット」（318 ページ参照）が有効な場合にのみ、入力可能になります。

「*管理者電話番号*」

管理責任者の電話番号を入力します（任意）。
E-mail フォーマットとして、「ITS フォーマット」（318 ページ参照）が有効な場合にのみ、入力可能になります。

「*装置 ID*」

この ID は、シリアル番号のように、サーバ ID に付加されます。
E-mail フォーマットとして、「Fujitsu REMCS フォーマット」が有効な場合にのみ、入力可能になります。

「*送信元サーバ URL*」

ある条件で、サーバがアクセスできる URL を指します。URL を手入力しなければなりません。
E-mail フォーマットとして、「標準メール」が有効な場合にのみ、入力可能になります。

➤［*適用*］ボタンをクリックして、設定を保存してください。

7.13 ユーザー管理 – ユーザーの管理

「ユーザー管理」エントリは、ローカルユーザー管理のページだけでなく、ディレクトリサービスでのユーザー管理のためのディレクトリサービス構成（***LDAP 構成***）のリンクを含みます：

– 311 ページの「iRMC S2 ユーザー iRMC S2 のローカルユーザー管理」

– 321 ページの「ディレクトリサービス設定（LDAP） – iRMC S2 のディレクトリサービスの設定」

7.13.1 iRMC S2 ユーザー – iRMC S2 のローカルユーザー管理

「*iRMC S2* ユーザー」ページは、ユーザー設定に関する情報を含みます：すべての行が、ユーザー設定のためのデータを含んでいます。ユーザー名はリンク形式で表示されています。ユーザー名をクリックして、「ユーザー'ユーザー名 '設定」(314 ページ参照) 画面をオープンして、ユーザー設定の表示および修正を行ってください。

i　ユーザー ID 1 (“null user”) は、IPMI 標準のために予約されています。そのため、iRMC S2 のユーザー管理に使用することはできません。

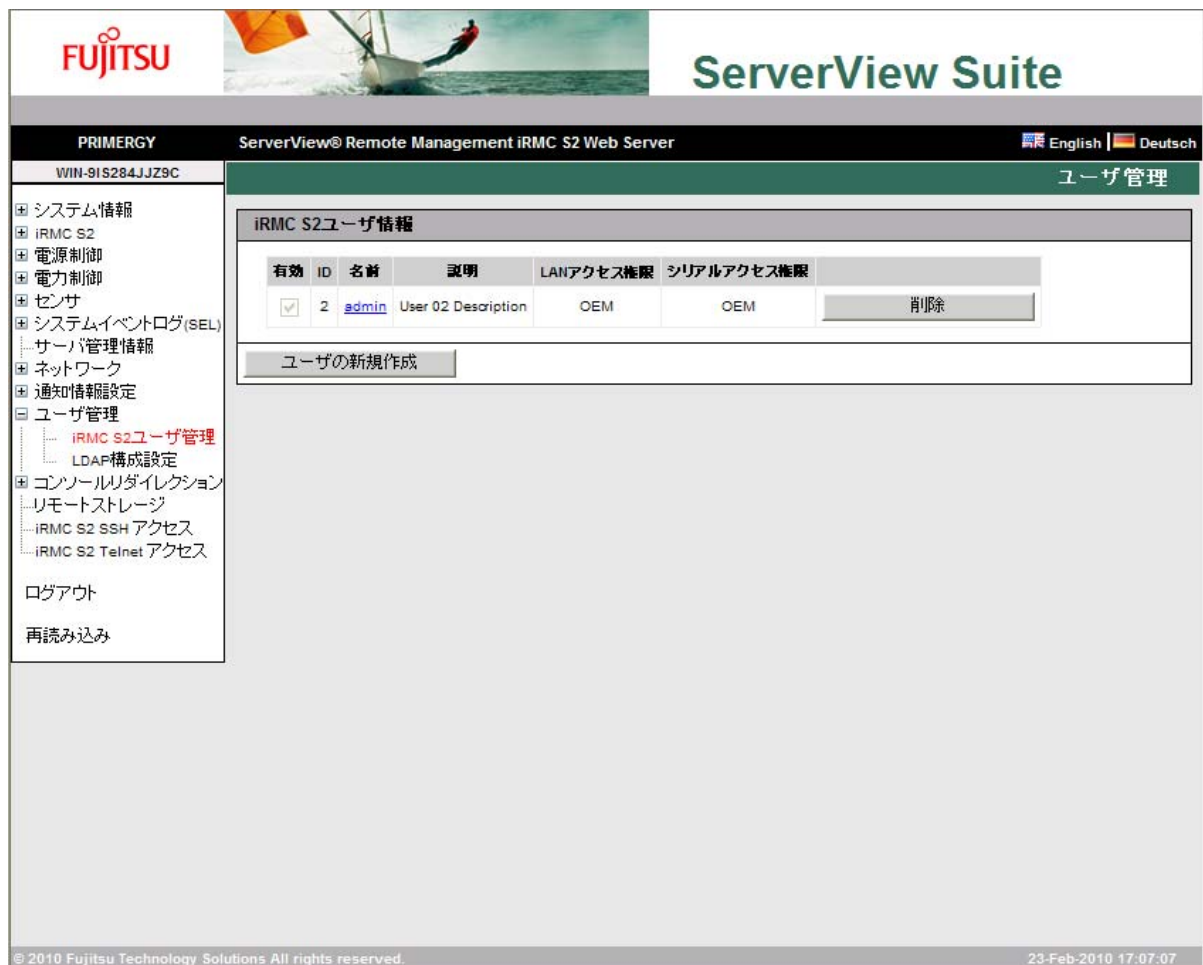



図 163 : ユーザー管理ページ

[*削除*]

ユーザー管理のテーブルは、[削除] ボタンをそれぞれのユーザーの後に含んでいます。

[*新規ユーザー*]

このボタンをクリックすると、「新規ユーザーの構成」ページ (313 ページ) 参照がオープンします。このページで、新規ユーザーを設定することができます。

7.13.1.1 新規ユーザーの構成 – 新規ユーザーの設定

「*新規ユーザーの構成*」ページを使って、新規ユーザーの基本設定を行うことができます。

「*新規ユーザーの構成*」ページ（315 ページの「ユーザー ‘ユーザー名 ’ 設定」ページの下）に、このフィールドの説明が記載されています。

図 164 に、“User3” という名前のユーザー設定の方法を示します。

図 164 ：ユーザー管理－新規ユーザーの構成ページ

7.13.1.2 ユーザー ' ユーザー名 ' 設定 – ユーザー設定（詳細）

「*ユーザー' ユーザー名 ' 設定*」ページを使って、ユーザー設定の表示、修正および拡張を行うことができます。図 165 に図 164 で作成されたユーザーの設定を示します。

ユーザー名の後ろの括弧内にユーザー ID が表示されています。

図 165 ：ユーザー管理－ユーザー名設定ページ

iRMC S2 ユーザー情報－ユーザークセスデータの設定

「*iRMC S2 ユーザー情報*」グループを使って、ユーザーのアクセス情報の設定を行うことができます。

iRMC S2ユーザ情報	
ユーザを有効にする:	☑
名前:	admin
パスワード:	••••••••••••••••••••
確認用パスワード:	
説明:	User 02 Description
使用シェル(Textアクセス):	Remote Manager
適用	

図 166 ： ユーザー管理－ユーザー名設定ページ、iRMC S2 ユーザー情報

「*ユーザーを有効にする*」
このオプションを無効に設定するとユーザーをロックすることができます。

「*名前*」
ユーザー名を入力してください。

「*パスワード*」
パスワードを入力してください。

「*パスワード確認*」
確認のため、ここにパスワードを再入力してください。

「*説明*」
ここに構成したユーザーの一般的な説明を入力してください。

「使用シェル（*Text* アクセス）」
ユーザーシェルを選択してください。
次のオプションを選択できます：

– 「SMASH CLP」
381 ページの「コマンドラインシェルの起動 ... – SMASH CLP シェルの起動」の節を参照してください。

– 「Remote Manager」
361 ページの「 Telnet/SSH アクセス（Telnet/SSL での管理）」の章を参照してください。

– 「IPMI Basic Mode」

– 「IPMI Terminal Mode」

– 「None」

➢［適用］ボタンをクリックして、設定を有効にしてください。

アクセス権限／許可－ユーザークセス権限の設定

「*権限／許可*」グループを使って、アクセス権限グループの設定を行うことができます。

権限/許可

LANアクセス権限: OEM
シリアルアクセス権限: OEM
ユーザ アカウント変更権限: ☑
iRMC S2設定変更権限: ☑
AVR使用権限: ☑
リモート ストレージ使用権限: ☑
適用

図 167 ： ユーザー管理－ユーザー名設定ページ、権限／許可

「*LAN アクセス権限*」
ここで、ユーザーに LAN アクセス権限を付与することができます

– 「User」
– 「Operator」
– 「Administrator」
– 「OEM」

許可とアクセス権限グループの関係については、56 ページの「ユーザー権限」の節を参照してください。

「*シリアルアクセス権限*」
ここで、ユーザーにシリアルアクセス権限を付与することができます :「LAN アクセス権限」にも、同じアクセス権限グループを設定することができます。

アクセス権限グループの許可に加えて、ユーザーにアクセスグループ権限外の以下の許可を付与することができます。

「ユーザーカウント変更情権限」
ローカルユーザー設定データにアクセスできる許可を付与します。

「*iRMC S2 設定変更権限*」
iRMC S2 設定を実行できる許可を付与します。

「*AVR 使用権限*」

ビデオリダイレクションに関する参照のみ可能および全体制御可能モードを設定する許可を付与します。

「リモートストレージ使用権限」

リモートストレージ機能の利用に関する許可を付与します。

➤［*適用*］ボタンをクリックして、設定を有効にしてください。

ファイルからのユーザー **SSHv2** 公開認証鍵のアップロード

「ファイルからのユーザー *SSHv2* 公開認証鍵のアップロード」グループを使って、ローカルファイルからのユーザーの SSHv2 公開鍵の登録を行うことができます。

ファイルからのユーザ SSHv2 公開認証鍵のアップロード(このユーザに割り当てられた認証鍵は存在しません)
SSHv2 公開認証鍵ファイル: [ ] 参照...
アップロード

図 168 : ユーザー管理－ユーザー名構成ページ、ファイルからのユーザー SSHv2 公開認証鍵のアップロード

iRMC S2 ユーザーの SSHv2 公開鍵認証に関する詳しい情報は、62 ページの「iRMC S2 ユーザーの SSHv2 公開鍵認証」を参照してください。

E-mail 構成－ユーザー特有の電子メール設定

「*E-mail* 構成」グループを使って、ユーザー特有の E-mail 送信フォーマットを行うことができます。

E-mail構成

E-Mailを有効にする: ☐
Mailフォーマット選択: 標準メール
優先Mailサーバ: 自動選択
送信先E-mailアドレス: User02@domain.com

事象毎のMail送信設定

Fan Sensors:	警告以上	Temperature Sensors:	警告以上
Critical Hardware Errors:	すべて送信	System Hang:	危険以上
POST Errors:	すべて送信	Security:	警告以上
System Status:	送信しない	Disk Drivers & Controllers:	危険以上
Network Interface:	警告以上	Remote Management:	危険以上
System Power:	警告以上	Memory:	危険以上
Other:	送信しない		

適用 テスト

図 169 ：ユーザー管理－ユーザー名設定ページ、E-mail 構成

「*E-mail を有効にする*」
ユーザーに電子メールによる情報を送信するか否かを設定します。

「*E-mail フォーマット選択*」
選択された E-mail フォーマットによって、「E-mail 通知－ E-mail フォーマットの設定グループ」(318 ページ参照)、を使って設定を行うことができます。

次の E-mail フォーマットがサポートされています：

– 「標準メール」
– 「題名固定」
– 「ITS フォーマット」（未サポート）
– 「FujitsuREMCS フォーマット」

「*優先 Mail サーバ*」
参照メールサーバを選択してください。
次のオプションを選択することができます：

– 「自動選択」

電子メールの送信に失敗した場合、例えば、プライマリメールサーバが稼動していない場合、ただちに、電子メールをセカンダリメールサーバに送信します。

– 「プライマリ」

プライマリ SMTP サーバ（307 ページ参照）として構築されたメールサーバのみを使用します。

– 「セカンダリ」

セカンダリ SMTP サーバ設定（308 ページ参照）として構築されたメールサーバのみを使用します。

i 電子メール送信エラーは、イベントログに記録されます。

「*送信先 E-mail アドレス*」
電子メールを受信者の電子メールアドレスを入力します。

「*事象毎の Mail 送信設定*」

ここでは、どのシステムイベントが iRMC S2 ユーザーに電子メールで通知されるのかを 設定します。

すべての iRMC S2 のイベントログを通知グループに設定する必要があります。

個々のイベントグループについて次の設定が可能です：

「送信しない」

この通知グループについては、通知されません。

「危険以上」

iRMC S2 は、システムイベントログに「危険以上」と記録されるイベントについて、ユーザーに電子メールで通知します。

「警告以上」

iRMC S2 は、システムイベントログに「軽度」、「重度」、あるいは、「危険」と記録されるイベントについて、ユーザーに電子メールで通知します。

「すべて送信」

iRMC S2 は、システムログに記録されるすべてのイベントについて、ユーザーに電子メールで通知します。

➢［適用］ボタンをクリックして、設定を有効にしてください。

7.13.2 ディレクトリサービス設定（LDAP）－ iRMC S2 のディレクトリサービ スの設定

ディレクトリサービスでユーザー管理を行う（76 ページ参照）ために、iRMC S2 の適切な構成を「ディレクトリサービス構成」内に行わなければなりません。

現在、iRMC S2 LDAP は、次のディレクトリサービスをサポートしています： Microsoft Active Directory 、および Open LDAP

以下の文字は、LDAP 検索のためのメタキャラクタとして予約されています： * 、\ 、& 、| 、! 、= 、< 、> 、~ ：

Relative Distinguished Names (RDN) の構成にこれらの文字を使うことはできません。

FUJITSU　ServerView Suite

PRIMERGY　ServerView® Remote Management iRMC S2 Web Server　English　Deutsch

WIN-TOMOWNBGIY5　ディレクトリ サービス構成

システム情報
iRMC S2
電源制御
電力制御
センサ
システムイベントログ(SEL)
サーバ管理情報
ネットワーク
通知情報設定
ユーザ管理
iRMC S2ユーザ管理
LDAP構成設定
コンソールリダイレクション
リモートストレージ
iRMC S2 SSH アクセス
iRMC S2 Telnet アクセス
ログアウト
再読み込み

ディレクトリ サービス構成設定

LDAPを有効にする: ☑
LDAP SSL接続を有効にする: ☐
ローカルIDでのログインを無効にする ¹: ☐
常にSSLログインを使用する ²: ☑
ディレクトリ サーバ タイプ: Active Directory
LDAPサーバ 1: test.fjlab.com
LDAPサーバ 2: 10.21.136.XXX
ドメイン名: domain.com
Base DN: DC=domain,DC=com
Base DN配下のグループディレクトリ:
Dept. name: DeptX

適用

注(1): 警告：この設定を行うとディレクトリサーバがアクセス不可能な場合にはログインできません!
注(2): LDAPが無効な場合でもhttpsログインを使用します.

ディレクトリ サービス アクセス構成

LDAP認証ユーザ名: LDAPuserName
LDAP認証パスワード: ••••••••••••••••••••
確認用パスワード:

適用　LDAP アクセステスト

ディレクトリ サービスE-mail警告構成

LDAP E-mail警告を有効にする: ☐
LDAP警告テーブルを更新する: 0 時間

適用

© 2010 Fujitsu Technology Solutions All rights reserved.　24-Feb-2010 14:49:54

図 170 ：ディレクトリサービス構成ページ（LDAP 構成）

「*LDAP を有効にする*」

このオプションで、iRMC S2 が、LDAP を通してディレクトリサービスにアクセスでき るか否かを設定します。LDAP を通してのディレクトリサービスへのアクセスは、「LDAP を有効にする」オプションが有効な場合に利用できます。

「LDAP を有効にする」オプションがチェックされた場合、ログイン情報 （210 ページ参照）は、常に Web ブラウザと、iRMC S2 の間を、SSL 暗号化されて送信されます。

「*LDAP SSL 接続を有効にする*」

このオプションがチェックされた場合、iRMC S2 とディレクトリサーバ間のデータ送信は、SSL 暗号化を利用して行われます。

「LDAP SSL 接続を有効にする」は、iRMC S2 Web インターフェースページがオープン時に SSL 保護されているか否かに影響を与えません。

「LDAP SSL 接続を有効にする」は、ドメインコントローラ認証がインストールされている場合に、有効にすることができます。

「*ローカル ID でのログインを無効にする*」

このオプションを有効にした場合、iRMC S2 のローカルユーザー認証はロックされ、ディレクトリサービスによるユーザー認証のみが有効になります。

注意！

「ローカル ID でのログインを無効にする」が有効になっていて、ディレクトリサービスへの接続が不可能な場合、iRMC S2 へのログインはできなくなります。

「*常に SSL ログインを使用する*」

オプションは、LDAP が無効になっている場合に、有効になります。

このオプションを有効にした場合、LDAP オプションが無効になっていても、HTTP SSL-secured ログインページが常に利用されます。「常に *SSL* ログインを使用する」を有効にせず、かつ、LDAP が無効になっている場合は、簡易ユーザー認証がログインに使用されます。

「*ディレクトリサーバタイプ*」
ディレクトリサーバとして使われるタイプを指します：
次のディレクトリサービスがサポートされています：

– 「Active Directory」：マイクロソフト社 Active Directory
– 「Novell」：ノベル社 eDirectory（未サポート）
– 「OpenLDAP」：OpenLDAP

➢ ［*適用*］ボタンをクリックして、設定を有効にしてください。

選択したディレクトリサービスによって、異なった入力フィールドが表示されます：

– 「*Active Directory*」については、324 ページの「マイクロソフト社 Active Directory の iRMC S2 用設定」を参照してください。

7.13.2.1 マイクロソフト社 Active Directory の iRMC S2 用設定

「*Active Directory*」を選択し、[*適用*] ボタンをクリックすると、「ディレクトリサービス構成」ページが表示されます .

図 171 ：ディレクトリサービス構成： マイクロソフト社 Active Directory の仕様

入力項目ついては、図 171 に例を表示します。107 ページの「Microsoft Active Directory による iRMC S2 ユーザー管理」を参照してください。

次の手順で行ってください：

➤「ディレクトリサービス構成設定」グループの設定を完成させてください：

ディレクトリ サービス構成設定	
LDAPを有効にする:	☐
LDAP SSL接続を有効にする:	☐
ローカルIDでのログインを無効にする:	☐
常にSSLログインを使用する:	☐
ディレクトリ サーバ タイプ:	Active Directory
LDAPサーバ 1:	0.0.0.0
LDAPサーバ 2:	0.0.0.0
ドメイン名:	domain.com
Base DN:	DC=domain,DC=com
Base DN配下のグループディレクトリ:	
Dept. name:	department
適用	

図 172 ：ディレクトリサービス設定：マイクロソフト社 Active Directory の仕様

「*LDAP サーバ 1*」
LDAP ディレクトリサービスとして利用するサーバの IP アドレスあるいは DNS 名を入力してください。

「*LDAP サーバ 2*」
「*LDAP サーバ 1*」に不具合が生じた場合のバックアップサーバとして、LDAP ディレクトリサーバの IP アドレスあるい DNS 名を入力してください。

「*ドメイン名*」
ディレクトリサーバの DNS パス名を入力してください。

「 Base DN 」
「 *Base DN* 」は、「ドメイン名」から、自動的に設定されます。

「*Department Name*」
「*Department Name*」は、ディレクトリサービスで、ユーザー許可および警告ロールを決定するために使用されます。Department X サーバと Department Y サーバでは、異なる許可を持つことになります（90 ページの 図 27 参照）。

➤［*適用*］ボタンをクリックして、設定を有効にしてください。

➢「ディレクトリサービスアクセス構成」グループで、LDAP アクセスを構成します。

i この設定は、ディレクトリサービスでのユーザー認証において、警告通知を出す際に必要となります。警告通知が無効になっている場合、「ディレクトリサービスアクセス構成」グループは利用できません。

ディレクトリ サービス アクセス構成

LDAP認証ユーザ名: LDAPuserName

LDAP認証パスワード: ••••••••••••••••••••

確認用パスワード:

適用 LDAP アクセステスト

図 173 :「マイクロソフト社 Active Directory」ディレクトリサービスアクセス構成

「*LDAP 認証ユーザー名*」

LDAP サーバにログオンするときの iRMC S2 ユーザー名を入力してください。

「*LDAP 認証パスワード*」

LDAP サーバ認証用のパスワードをユーザー名の下に入力してください。

「*パスワード確認*」

「*LDAP* 認証パスワード」の下に確認のため、パスワードを再度入力してください。

［*LDAP アクセステスト*］

LDAP ディレクトリサーバへのアクセスデータをチェックし、LDAP の状況を表示します（図 174 参照）。

i　このテストは、基本アクセスデータ（「LDAP サーバが存在するか」あるいは 「ユーザーは設定されているか」）を確認するもので、ユーザー認証のすべて を確認するものではありません。

ディレクトリ サービス アクセス構成

LDAP 状態: 無効のLDAPサーバ
LDAP認証ユーザ名: LDAPuserName
LDAP認証パスワード: ••••••••••••••••••••
確認用パスワード:

適用　LDAP アクセステスト　LDAP状態のリセット

図 174：「マイクロソフト社 Active Directory」：LDAP サーバへの接続状況

➢［*LDAP* 状態のリセット］ボタンをクリックして、画面への表示をリセットしてください。

➢［適用］ボタンをクリックして、設定を有効にしてください。

➢「ディレクトリサービス *E-mail* 警告構成」を使って、ディレクトリサービスを使用した電子メール通知の設定を行ってください。

ディレクトリ サービスE-mail警告構成

LDAP E-mail警告を有効にする:
LDAP警告テーブルを更新する: 0 時間

適用

図 **175**：ディレクトリサービス **E-mail** 警告構成

「***LDAP E-mail*** 警告を有効にする」

ディレクトリサービスを使用した電子メール通知を可能にします。

「***LDAP*** 警告テーブルを更新する」

ディレクトリサービスを使用した電子メールテーブルが更新される間隔を定義してください（**158** ページ参照）。「**0**」を設定すると、テーブルは更新されなくなります。

➢［*適用*］ボタンをクリックして、設定を有効にしてください。

7.13.2.2 ノベル社 eDirectory ／ OpenLDAP の iRMC S2 用設定（未サポート）

「Novell」あるいは「OpenLDAP」を選択して、［適用］ボタンをクリックすると、次の「ディレクトリサービス構成」ページが表示されます。

「ディレクトリサービス構成」ページは、ノベル社 eDirectory および OpenLDAP について、同じ内容です。

図 176：ディレクトリサービス構成：ノベル社 eDirectory ／ OpenLDAP の仕様

入力項目については、図 176 に例を表示します。120 ページの「Novell eDirectory によるグローバル iRMC S2 ユーザー管理」を参照してください。

次の手順で行ってください：

➢「 Global Directory Service Configuration（ディレクトリサービス設定）」グループを完成させてください:

ディレクトリ サービス構成設定

LDAPを有効にする: ☑
LDAP SSL接続を有効にする: ☐
ローカルIDでのログインを無効にする: ☐
常にSSLログインを使用する: ☑
ディレクトリ サーバ タイプ: Novell
LDAPサーバ 1: test.fjlab.com
LDAPサーバ 2: 10.21.136.XXX
Dept. name: DeptX
Base DN: ou=myorganization,ou=mycompany
Base DN配下のグループディレクトリ:
User Search Context:

適用

図 177 ：ディレクトリサービス構成：マイクロソフト社 Active Directory の仕様

「*LDAP サーバ 1*」

LDAP ディレクトリサーバとして利用するサーバの IP アドレスあるいは DNS 名を入力してください。

「*LDAP サーバ 2*」

「LDAP サーバ *1*」に不具合が生じた場合のバックアップサーバとして、LDAP ディレクトリサーバの IP アドレスあるいは DNS 名を入力してください。

「*Department Name*」

「Department Name」は、ディレクトリサービスで、ユーザー許可および警告ロールを 決定するために使用されます。Department X サーバと Department Y サーバでは、異なる許可を持つことになります（90 ページの 図 27 参照）。

「*Base DN*」

「*Base DN*」は、eDirectory あるいは Open LDAP サーバの完全な分類名を示し、そして、OU (Organizational Unit) *iRMCgroups* を含むツリーあるいはサブツリーを表します。この「Base DN」は、LDAP 検索の開始点を示します。

「*Base DN 配下のグループディレクトリ*」
　　「iRMCgroups（*iRMC* グループ）」の組織的構成のパス名は、「Base DN」のサブツリーを構成します（DN グループ検索方式）。

「*User Search Context*」
　　「Users」の組織的構成のパス名は、「Base DN」のサブツリーを構成します（ユーザー検索方式）。

➢［*適用*］ボタンをクリックして、設定を有効にしてください。

➢「ディレクトリサービスアクセス構成」グループで、LDAP アクセスを構成します。

ディレクトリ サービス アクセス構成

LDAP認証パスワード: ••••••••••••••••••••
確認用パスワード:
Principal User DN: cn=myprincipal,ou=people
Principal User DNに Base DNを追加する:
Bind DN: OU=
拡張ユーザ ログイン:
適用　LDAP アクセステスト

図 178 :「マイクロソフト社 Active Directory」: ディレクトリサービスアクセス構成

「*LDAP 認証パスワード*」
　　「プリンシパルユーザー」のパスワードを、LDAP サーバでの認証に入力してください。

「*パスワード確認*」
　　「LDAP 認証パスワード」の下に確認用のパスワードを繰り返し、入力してください。

「*Principal User DN*」
　　完全な構成名、例えば、iRMC S2 で作成されたユーザー ID（プリンシパルユーザー）の 属性オブジェクトパスの完全な情報を問い合わせる際に、iRMC S2 には、LDAP サーバ からの iRMC S2 ユーザーの問い合わせアクセス権限が必要です。

「*Principal User DN* に *Base DN* を追加する」
　　このオプションを有効にした場合は、BN ベースの下に「プリンシパルユーザー DN」を 設定するする必要はありません。この場合、DN ベースは、「Base DN」の下の「ディレクトリサービス構成」グループで設定されます。

「*Bind DN*」
　　「*Bind DN*」は、LDAP 認証において使用されるプリンシパルユーザー DN を示します。

「*拡張ユーザーログイン*」

ユーザーがログインする際の柔軟さを拡張することができます。
「拡張ユーザーログイン」を選択し、[適用] ボタンで有効にした場合、「ユーザーログイン検索フィルタ」フィールドが、標準のログイン画面に追加表示されます。

このオプションの有効化は、LDAP 構文に詳しい方のみご利用ください。不正な検索フィルタを設定および有効にした場合、「拡張ユーザーログイン」オプションが無効になるまで、iRMC S2 へのログインは、ディレクトリサービスを使用したログインしか使えなくなります。

図 179 :「拡張ユーザーログイン」用 LDAP 検索フィルタ

ログイン時には、「%s"」プレースホルダが、ディレクトリサービスを使用したログインに関連した内容に置き換わります。標準フィルタを「cn=」に変えて、他の属性に置き換 えることができます。すべてのディレクトリサービスを使用したログインは、この検索フィルタの評価基準を満たす場合に、iRMC S2 へのログインが許可されます。

注意！
このオプションの有効化は、LDAP 構文に詳しい方のみご利用ください。不正な検索フィルタを設定および有効にした場合、「拡張ユーザーログイン」オプションが無効になるまで、iRMC S2 へのログインは、ディレクトリサービスを使用したログインしか使えなくなります。

「*LDAP アクセステスト*」
LDAP ディレクトリサーバへのアクセスデータをチェックし、LDAP の状況を表示します（図 174 参照）。

> **i** このテストは、基本アクセスデータ（「LDAP サーバが存在するか」あるいは「ユーザーは構成されているか」）を確認するもので、ユーザー認証のすべてを確認するものではありません。

ディレクトリ サービス アクセス構成

LDAP 状態: 無効のLDAPサーバ
LDAP認証ユーザ名: LDAPuserName
LDAP認証パスワード: ••••••••••••••••••••
確認用パスワード:

適用　LDAP アクセステスト　LDAP状態のリセット

図 180：「eDirectory ／ OpenLDAP」: LDAP サーバへの接続状況

➢［*LDAP* 状態のリセット］ボタンをクリックして、画面への表示をリセットしてください。

➢［適用］ボタンをクリックして、設定を有効にしてください。

➢「ディレクトリサービス *E-mail* 警告構成」を使って、ディレクトリサービスを使用した電子メール通知の設定を構成します。

図 181：ディレクトリサービス E-mail 警告構成

「*LDAP Email* 通知を有効にする」
ディレクトリサービスを使用した電子メール通知を可能にします。

「*LDAP* 警告テーブルを更新する」
電子メールテーブルが更新される間隔を定義してください（158 ページ参照）。「 0 」を設定すると、テーブルは更新されなくなります。

➢［適用］ボタンをクリックして、設定を有効にしてください。

7.14 コンソールリダイレクション－コンソールのリダイレクト

次のページでコンソールリダイレクションについて説明します。

– 333 ページの「 BIOS テキストコンソール－テキストコンソールのリダイレクションの設定と開始」

– 344 ページの「ビデオリダイレクション－ビデオリダイレクション（AVR ）の開始」

7.14.1 BIOS テキストコンソール－テキストコンソールのリダイレクションの 設定と開始

「BIOS テキストコンソール」ページを使って、テキストコンソールのリダイレクションの設定および開始を行うことができます。

テキストコンソールリのダイレクションは、BIOS（38 ページの「 BIOS/TrustedCore セットアップユーティリティによる LAN をとおしたテキストコンソールのリダイ レクションの設定」の節参照）でも構成することができます。

図 182 ：BIOS テキストコンソールページ

7.14.1.1 BIOS コンソールリダイレクションオプション－テキストコンソールリのダイレ クションの設定

「*BIOS* コンソールリダイレクションオプション」を使って、テキストコンソールリのダイレクションを設定することができます。

BIOSコンソール リダイレクション オプション

コンソール リダイレクションを有効にする !:	☐
コンソール リダイレクション モード:	標準
コンソール リダイレクション ポート:	COM1
シリアルポート ボーレート:	9600
シリアルポート フロー制御:	フロー制御なし
端末エミュレーション:	VT100 7Bit
シリアル 1 マルチプレクサ:	System

適用

図 183：BIOS テキストコンソールページー BIOS コンソールリダイレクションオプション

「*コンソールリダイレクションを有効にする*」
　このオプションは、コンソールリダイレクションを有効／無効に設定します。

i　オペレーティングシステムでも、BIOS 設定にかかわらず、テキストコンソールリのダイレクションを許可することができます。

「*コンソールリダイレクションモード*」
　この設定は、オペレーティングシステムが稼動中（BIOS POST フェーズ完了後）のコンソールリダイレクションの動作に影響します。342 ページの「 オペレーティングシステ ム稼動中のテキストコンソールリのダイレクション」の節を参照してください。

「*標準*」
　コンソールリダイレクションは、BIOS POST フェーズの後、終了します。

「*拡張*」
　コンソールリダイレクションは、BIOS POST フェーズが完了した後も有効になります。

「*コンソールリダイレクションポート*」
二つのシリアルポートが利用できます :「シリアル 1」および「シリアル 2」。

i LAN を経由したコンソールリダイレクションを行う場合は、「シリアル 1」が設定されている必要があります。

「シリアル 2」が選択された場合、接続は、モデムケーブルを通してのみ可能 となります。

「*シリアルポートボーレート*」
次のボーレートが設定可能です: 1200 、2400 、4800 、9600 、19200 、38400 、57600 、115200 bps

「*シリアルポートフロー制御*」
次の設定が可能です。
「フロー制御なし」
通信制御は行いません。

「*XON/XOFF (Software)* 」
通信制御がソフトウェアによって行われます。

「*CTS/RTS (Hardware)* 」
通信制御がハードウェアによって行われます。

「*端末エミュレーション*」
次の端末エミュレーションがサポートされています。
VT100 7Bit 、VT100 8Bit 、PC-ANSI 7Bit 、P C-ANSI 8 Bit 、VT100+、VT-UTF8

「*シリアル 1 マルチプレクサ*」
マルチプレクサの設定との一貫性を確認しています :

－ 「System」: システム
－ 「LAN」: iRMC S2

➢ ［*適用*］ボタンをクリックして、設定を有効にしてください。

7.14.1.2 テキストコンソールのリダイレクション（LAN 上のシリアル通信）－テキストコ ンソールリのダイレクションの開始

「テキストコンソールリのダイレクション（LAN 上のシリアル通信）」を使って、テキストコンソールリのダイレクションを開始することができます。

「テキストコンソールリのダイレクション（LAN 上のシリアル通信)」は、オペレーティングシステムあるいは BIOS が、テキストコンソールリのダイレクションに、「シリアルポート 1（COM1)」を使っていると仮定しています。

テキストコンソールのリダイレクション（LAN上のシリアル通信）

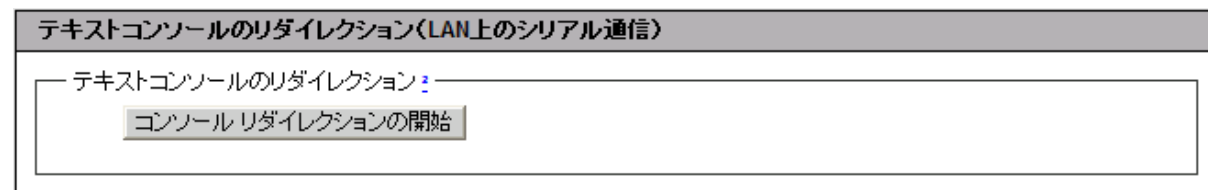
テキストコンソールのリダイレクション ?

[コンソール リダイレクションの開始]

図 184：テキストコンソールリのダイレクション（LAN 上のシリアル通信）

➢ ［*コンソールリダイレクションの開始*］ボタンをクリックして、テキストコンソールリのダイレクションを開始してください。

テキストコンソールリのダイレクション用の Java アプレットが開始されます（図 185 参照）：

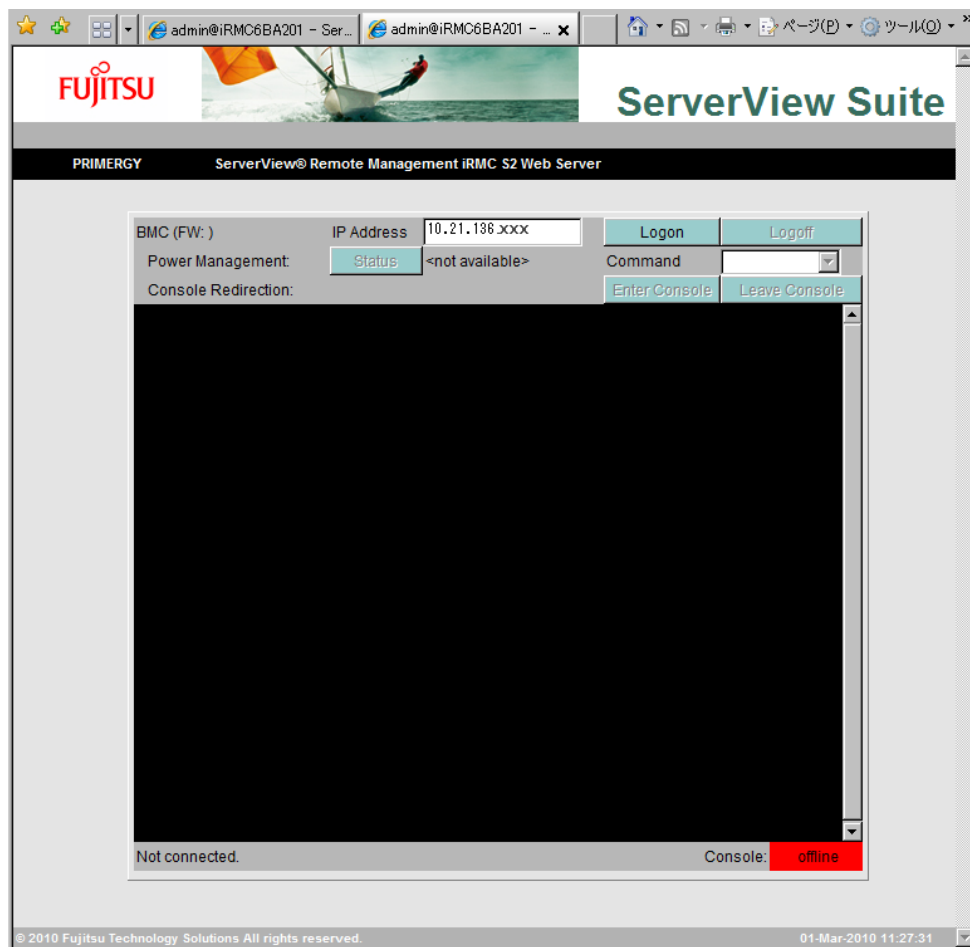



図 185 ： 電源管理およびテキストコンソールリのダイレクション（ログイン前）

➢ ［*Logon*］ボタンをクリックして、iRMC S2 にログインしてください。

iRMC S2 のユーザー名およびパスワードを入力するよう表示されます：

ServerView Remote Management Frontend 10.21.136.xxx

Username: admin

Password: •••••

Login　　Cancel

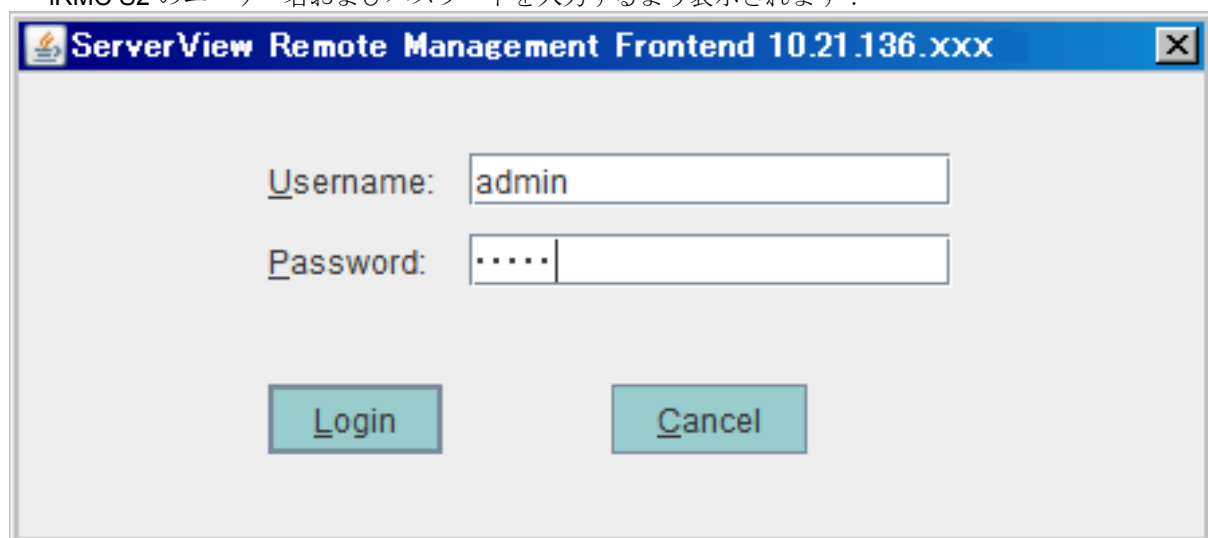



図 186 ：電源管理およびテキストコンソールリのダイレクションログイン画面

ユーザー名およびパスワードを入力し、［*Login*］ボタンをクリックしてください。
電源管理およびテキストコンソールリのダイレクション画面が表示されます。

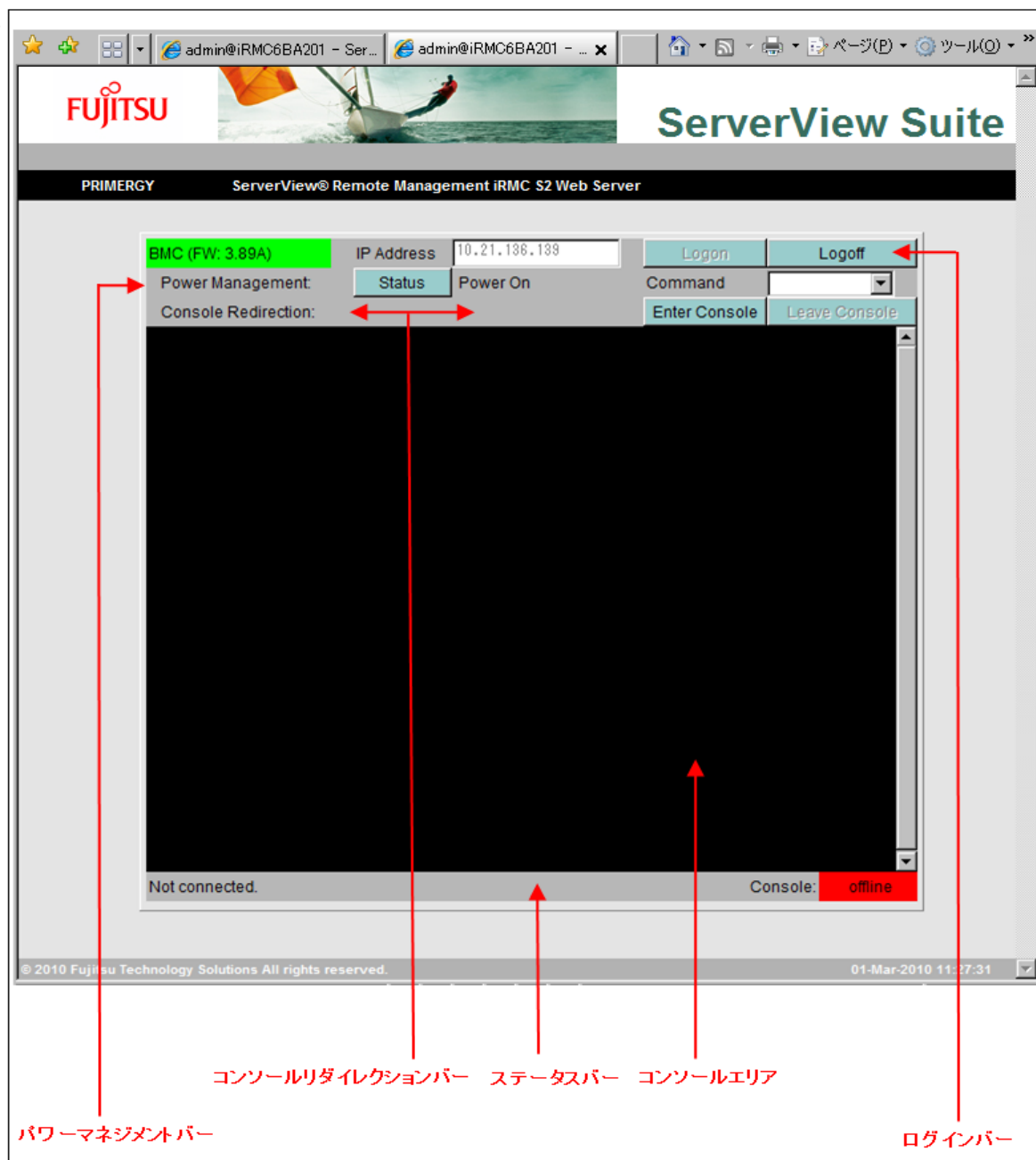



図 187：電源管理およびテキストコンソールリのダイレクション画面

コンソールリダイレクション画面に表示される項目の説明は以下の通りです。

「*Login bar*」
ログインバーは、iRMC S2 の IP アドレスおよび現状のファームウェアのバージョンを表示します。［Login］および［Logout］ボタンを使って、iRMC S2 にログインあるいはログアウトできます。

「*Power management bar*」
電源制御バーは、管理サーバの電源状態の情報を表示します。［Status］ボタンをクリックして、表示を更新することができます。
「Command」ドロップダウンリストを使って、管理サーバの IPMI コマンドを選択および実行することができます（341 ページ参照）。これを行うために、コンソールに接続する必要はありません。

「*Console redirection bar*」
コンソールリダイレクションバー内の［ Enter Console （コンソール表示）］および［ Leave Console （コンソール非表示）］ボタンを使って、コンソールエリアを表示／非表示に切り替えることができます。

「*Console area*」
コンソールエリアに、リダイレクトされたテキストコンソールが表示されます。

「*Status bar*」
ステータスバーは、iRMC S2 の IP アドレスおよびコンソールリダイレクションのポート番号を表示します。それに加え、ステータスバーは、コンソールリダイレクションのオンライン／オフラインの状態を表示します。

➢［*Enter Console*］ボタンをクリックしてください。

コンソールに接続され、コンソールエリアで直接入力するか、「Command」ドロップダウンリストから選択し、必要なコマンドを実行することができます（IPMI コマンドのみ）

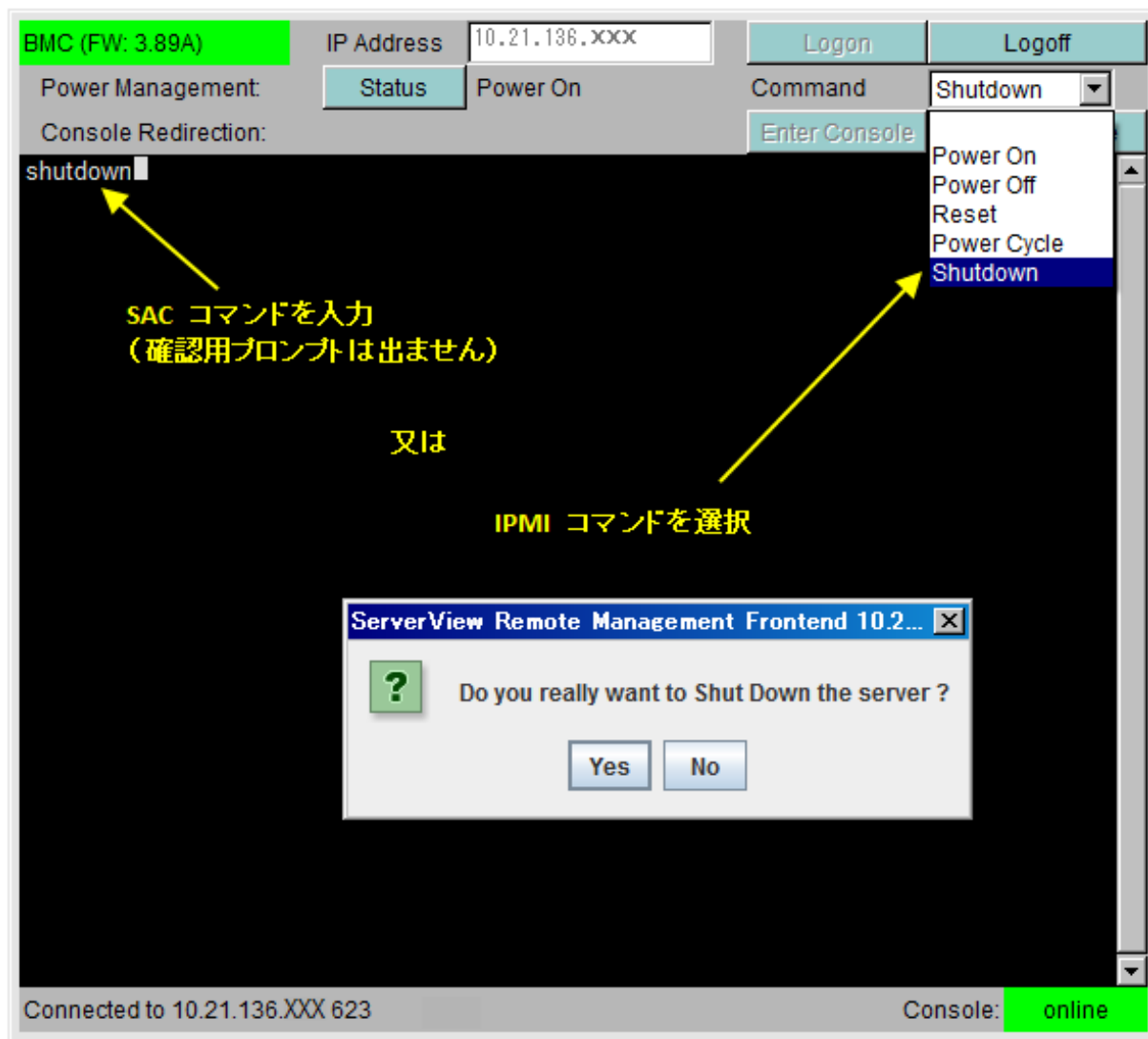



図 188：SAC あるいは IPMI コマンドをコンソールからの入力

IPMI コマンドの説明

「*Power On*」　サーバの電源を投入します。
「*Power Off*」　サーバの電源を切断します。
「*Reset*」　オペレーティングシステムの状況にかかわらず、サーバを再起動します（コールドスタート）
「*Power Cycle*」　サーバの電源切断から、およそ 5 秒経過後、電源投入を行います。
「*Shutdown*」　サーバを適切にシャットダウンし、電源を切断します。

➢ コンソールとの接続を閉じる場合には、［ *Leave Console* （コンソール非表示）］ボタンをクリックしてください。

7.14.1.3 オペレーティングシステム稼働中のテキストコンソールリのダイレクション

管理サーバのオペレーティングシステムによっては、BIOS POST フェーズ後もコンソールリダイレクションを利用しつづけることができます。

DOS

条件：
コンソールリダイレクションの BIOS 設定が、「Enhanced」に設定されていなければなりません（333 ページの「BIOS テキストコンソール－テキストコンソールのリダイレ クションの設定と開始」参照）

管理サーバが、ServerView Suite diagnosis ソフトウェアを起動している場合は、コンソールリダイレクションを使って、ServerView Suite diagnosis を操作することができます。ServerView Suite diagnosis に関する詳しい情報は、『RemoteView 5.0』ユーザーガイドを参照してください。

Windows Server 2003

Windows Server 2003 は、POST フェーズ後、自動的にコンソールリダイレクションを扱えるようにします。設定は必要ありません。オペレーティングシステムが起動中に、Windows Server 2003 SAC コンソールに切り替えます。

図 189：Windows Server 2003 SAC コンソール

Linux

Linux オペレーティングシステムでは、POST フェーズ後にコンソールリダイレクションを扱うために次の設定をしなければなりません。一度、構成すれば、リモートアクセスも可能になります。

必要な設定

設定は、プログラムのバージョンによって異なる場合があります。

SuSE and RedHat（SuSE は未サポート）

/etc/inittab ファイルの最後に次の行を追加してください：

xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0

RedHat

/etc/grub.conf ファイルのカーネルブートパラメータに以下を追加してください：

console=ttyS0,<baud-rate> console=tty0

SuSE (未サポート)

/boot/grub/menu.lst ファイルのカーネルブートパラメータに以下を追加してください：

console=ttyS0,<baud-rate> console=tty0

7.14.2 ビデオリダイレクション（AVR）－ビデオリダイレクション（AVR）の 開始

「*ビデオリダイレクション*（*AVR*）」ページを使って、グラフィカルなコンソールリダイレクションを開始することができます。ビデオリダイレクションの特徴は、管理サーバからのグラフィカルな出力をリモート管理端末に表示し、そして、リモート管理端末から管理サーバへのキーボードおよびマウスを使えるようにすることです。その結果、リモート管理端末で、管理サーバ上と同じ操作をすることができます。
ビデオリダイレクションは、同時に二人のユーザーが使用できます。片方のユーザーがサーバをフルコントロールしている場合（フルコントロールモード）、もう一方のユーザーは、キーボードおよびマウスの操作を見ることしかできなくなります（参照モード）。

iRMC S2 の「ビデオリダイレクション（AVR）」機能を使うためには、ライセンスキー（229 ページの「iRMC S2 へのライセンスキーのアップロード」参照）が必要です。

ビデオリダイレクションは、Java アプレットを利用しています。

図 190 ：ビデオリダイレクション（AVR）ページ

ASR スクリーンショットの作成

「スクリーンショット」ページを使って、
－管理サーバの現在の VGA 画面のスクリーンショットの取得、および、それを iRMC S2 のファームウェアに保存することができます。
－ iRMC S2 に保存されたスクリーンショットの表示を行うことができます、
－ iRMC S2 に保存されたスクリーンショットの削除を行うことができます。

スクリーンショット			
全画面表示	プレビュー	作成	削除

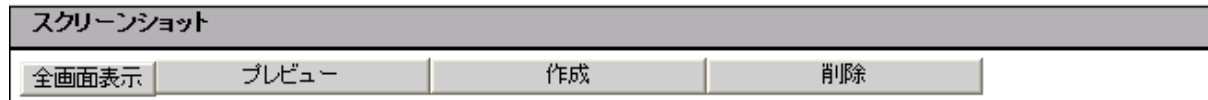



図 191 : ビデオリダイレクションのスクリーンショットの作成

> ASR イベント発生時（Windows では、特有なウォッチドッグイベントあるいは 管理サーバの「ブルースクリーン画面」発生時に）に自動的にスクリーンショットが作成されます。
>
> 最大「一つ」のスクリーンショット（作成日が新しいスクリーンショット）が、iRMC S2 のファームウェアに保存されます。

表示されるボタンをクリックして、以下の動作を行うことができます :

［*全画面表示*］
(スクリーンショットが既に保存されている場合にのみ、表示されます。)
スクリーンショットは、別のブラウザ画面に表示されます。

［*プレビュー*］
(スクリーンショットが既に保存されている場合にのみ、表示されます。)
「スクリーンショット」グループで、スクリーンショットのサムネイルが表示されます。

［*作成*］
現在のスクリーンショットを取得します。

［*削除*］
(スクリーンショットが既に保存されている場合にのみ、表示されます。)
iRMC S2 firmware 保存されたビデオスクリーンショットが、確認後、削除されます。

AVR 実行中セッション表－現在のビデオリダイレクションセッションの表示

「AVR 実行中セッション表」に、現在の稼働中のビデオリダイレクションアクティブセッションが表示されます。ビデオリダイレクションアクティブセッションが稼動していない場合、「 AVR Active Session Table（ビデオリダイレクションアクティブセッションテーブル）」は、表示されません。

二つのビデオリダイレクションアクティブセッションが稼動している場合、［切断］ボタンが、それぞれの接続の切断用に表示されます。

AVR実行中セッション表

番号	IPアドレス	ユーザ名	ユーザID	アクセス権限	ストレージ有効	コントロール取得可能	セッション状況	
1	10.21.136.105	admin	2	フルコントロール	Yes	Yes	確立済	切断
2	10.21.136.235	admin	2	表示のみ	No	Yes	確立済	切断

図 192 : AVR 実行中セッション表ー（二つのビデオリダイレクションアクティブセッションが有効な場合）

「*切断*」

［切断」ボタンをクリックすると、確認ダイアログが表示され、左側のボタンで、ビデオリダイレクションアクティブセッションを切断することができます。

i ［切断］ボタンを使って、他のユーザーのビデオリダイレクションアクティブセッションを切断することができます。自分自身のビデオリダイレクションアクティブセッションを閉じる場合には、ビデオリダイレクションの「拡張機能」メニューか ら、［Exit］ボタンを使用します（173 ページ参照）。

ビデオリダイレクションオプションー管理サーバ上のビデオリダイレクションセッション中の **USB** ポートの無効化

この機能は、一部の PRIMERGY サーバでサポートされていません。

「ビデオリダイレクションオプション中は *USB* ポートを無効化する」を使って、管理サーバ上で、ビデオリダイレクションセッション中に、どの USB ポートを無効にするかを設定することができます。

図 193 :「ビデオリダイレクションオプション」

「 *None*」

無効にする USB はありません。

「*Front USB*」
　　サーバの前面の USB ポートのみが使用不可能になります。

「 *Rear USB*」
　　サーバの背面の USB ポートのみが使用不可能になります。

「*Disable All*」
　　サーバのすべての USB ポートが無効化されます。

➤ ［*適用*］ボタンをクリックして、設定を有効にしてください。

サーバ側モニターサーバ側モニタの ON/OFF オプション

管理サーバ上モニタの状態は、「サーバ側のモニタ」の下に表示されます（161 ページの「サーバ側 のモニタ ON/OFF 機能」の節を参照）。

それに加え、以下の設定ができます。

– リモート管理端末から、サーバ側モニタの出力 ON/OFF が可能です、
– サーバ側モニタの電源は、ビデオリダイレクションセッションが開始され、ビデオリダイレクションセッション中は、自動的にシャットダウンされます。

図 194 ：ビデオリダイレクション（AVR）ページーサーバ側のモニタ

「*サーバ側モニタの出力を有効にする*」

このオプションを使って、以下のオプションを有効にすることができます：

– ビデオリダイレクションセッションのフルコントロールモード時において、「拡張機 能」メニューを使って、サーバ側モニタの出力を ON/OFF することができます （173 ページ参照）。

– 管理者あるいは **OEM** 許可を持ったユーザーは、［出力 OFF］／［出力 **ON**］切り替えボタンも使うことができます。この方法を使って、サーバ側モニタを電源 ON/OFF することができます（図 195 参照）。

図 195 ： ビデオリダイレクション（AVR）ページーサーバ側のモニタの出力 ON/OFF

– サーバ側モニタの電源を、ビデオリダイレクションセッションが開始され、ビデオリダイレクションセッション中に自動的にオフにするように設定することもできます （ビデオリダイレクション開始時のサーバーモニタの自動オフオプションを参照）。

サーバ側モニタオフの設定をしているセッションがない場合、ビデオリダイレクションセッションが終了するとサーバ側モニタは自動的に電源オンになります。

「AVR 開始時に自動的にサーバ側モニタ出力を OFF にする」

このオプションは、「サーバ側モニタの出力」が有効な場合のみ、有効になります。

オ
プションを有効にした場合、サーバ側モニタは、ビデオリダイレクションセッションが開始され、ビデオリダイレクションセッション中は自動的にオフになります。ビデオリダイレクションセッションが終了し、サーバ側モニタオフの設定をしているセッションがない場合、サーバ側モニタは自動的に電源オンになります。

ビデオリダイレクション複数の接続：

たとえ、ビデオリダイレクションセッション中にサーバ側モニタの出力をオンにしても（ビデオリダイレクションメニューの「拡張機能」あるいは「出力 ON」ボタンを使って）、新しいビデオリダイレクションセッションが開始されると、サーバ側モニタは自動的に電源オフになります。
サーバ側モニタは、ビデオリダイレクションセッションが終了すると自動的に電源オンになります。

➤ ［適用］ボタンをクリックして、設定を有効にしてください。

ビデオリダイレクション－ビデオリダイレクションの開始

「ビデオリダイレクション」を使って、ビデオリダイレクションを開始することができます。

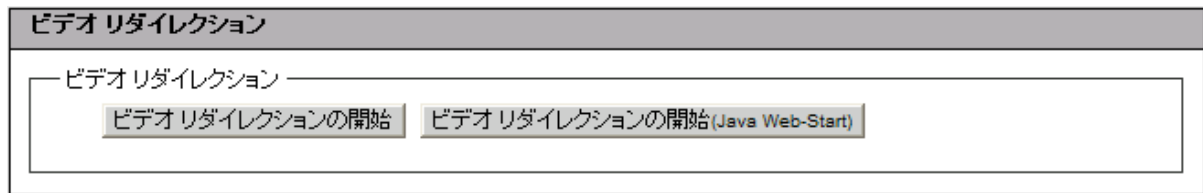



図 196：ビデオリダイレクションページーサーバ側モニタ

➢ ［ビデオリダイレクションの開始］あるいは［ビデオリダイレクションの開始（Java Web-Start)］ボタンをクリックして、2 番目のビデオリダイレクションセッションを開始することができます。

Java アプレットが、ビデオリダイレクションのために開始されます。

Java アプレットは、ビデオリダイレクション画面を参照モードで表示します。そして、管理サーバをフルコントロールするか、参照モードのままにするかを問い合わせます。

図 197：ビデオリダイレクション画面（参照モード）

➤［OK］ボタンをクリックして、サーバ管理のフルコントロールを取得してください。ビデオリダイレクション画面がオープンします（図 198 参照）。

現在のビデオリダイレクションセッションは AVR ビューモードです。
ユーザーは、どのモードを利用するのかについて、同意する必要があります。

➤［キャンセル］ボタンをクリックして、AVR ビューモードのままにします。

ビデオリダイレクションの利用を決定し、次の画面で、管理サーバにログインしてください。

図 198：ビデオリダイレクション画面（フルコントロールモード）

ビデオリダイレクション画面のメニューおよび特殊キーの同時使用は、156 ページの「ビデオリダイ レクション（AVR ）」の章に記載されています。

二つのビデオリダイレクションセッションは、「ビデオリダイレクション (AVR)」ページに次のように表示されます。

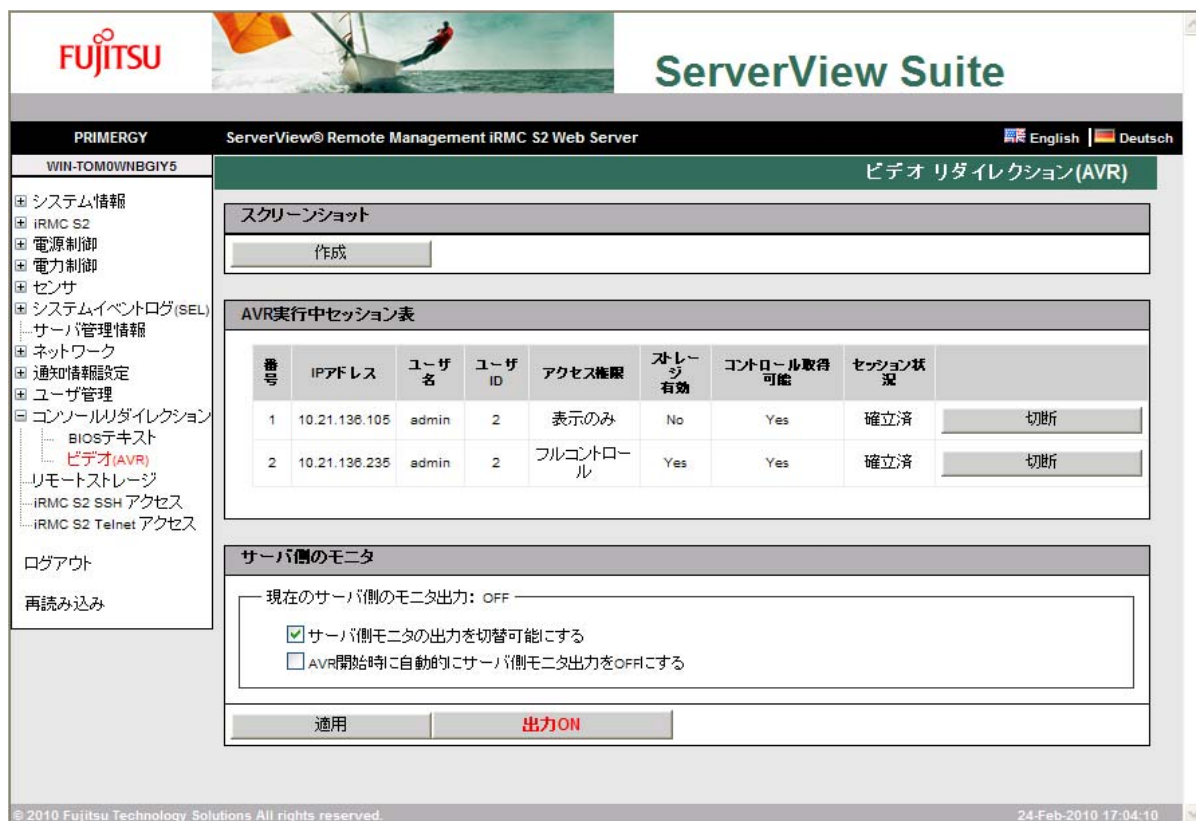



図 199：二つのビデオリダイレクションが有効な場合のビデオリダイレクション画面

［*切断*］

［切断］ボタンをクリックすると、確認ダイアログが表示され、ボタンの左側で、ビデオリダイレクションアクティブセッションを切断することができます。

［切断］ボタンを使って、他のユーザーのビデオリダイレクションアクティブセッションを切断することができます。自分自身のビデオコンソールリダイレクションアクティブセッションを閉じる場合には、ビデオコンソールリダイレクション画面の「拡張機能」メニューから、［Exit］ボタンを使用します（173 ページ参照）。

次の画面は、管理サーバが電源オフの場合に表示されます。

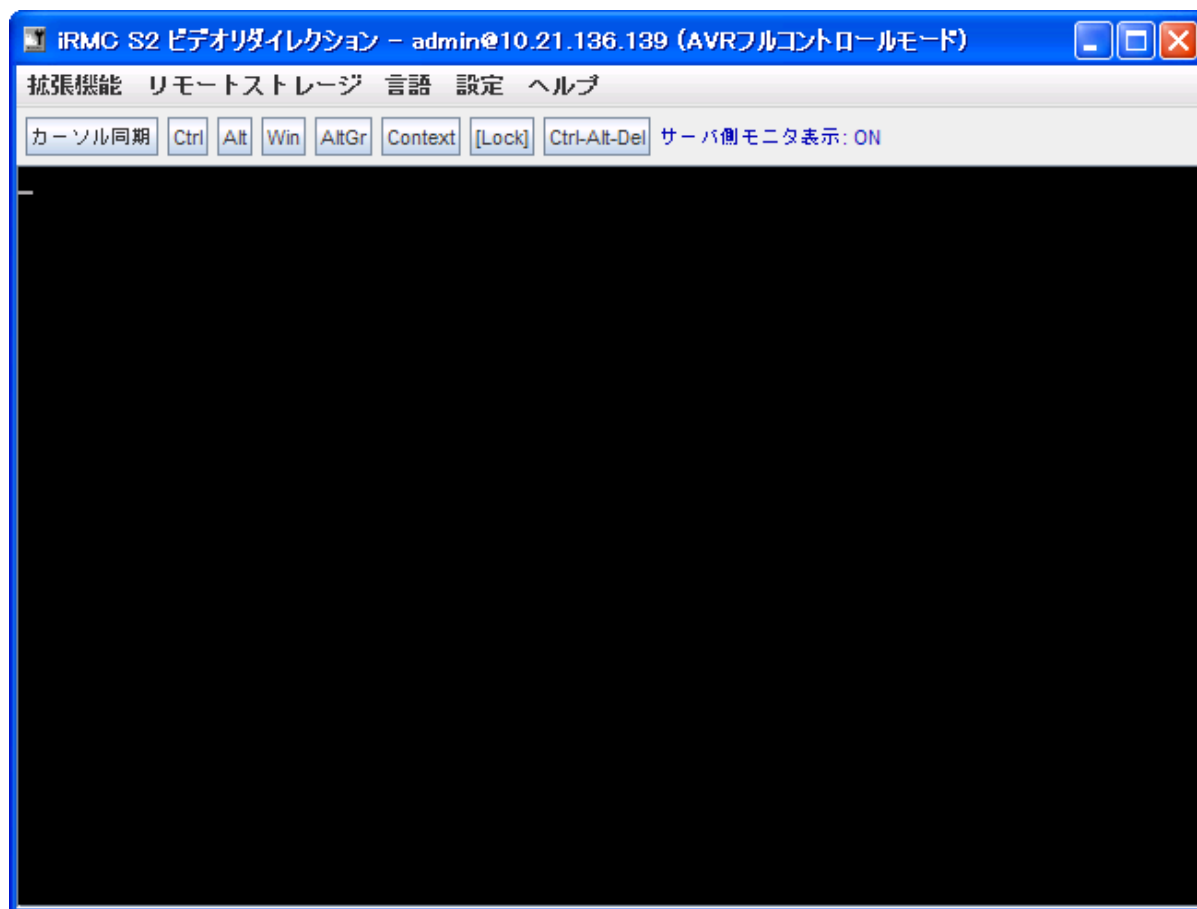



図 200：管理サーバが電源オフの場合のビデオリダイレクション画面

7.15 リモートストレージ

リモートストレージの特徴は、管理サーバにネットワーク上の他の場所に存在する「仮想」ドライブを提供することです。仮想ドライブとして、物理ドライブ（フロッピーディスクドライブあるいは CD-ROM ／ DVD-ROM）あるいは ISO イメージ（イメージファイル）を使うことができます。

iRMC S2 の「リモートストレージ」を使うためは、ライセンスキーが必要です　（231 ページ参照）。

リモートストレージの媒体として、以下の媒体が利用可能です：

– リモート管理端末上の物理ドライブあるいはイメージファイル（181 ページ参照）。イメージファイルはネットワークドライブ（たとえば、「 D: 」も D ドライブとして）も利用できます。

– リモートストレージサーバ経由のネットワーク上のイメージファイル（194 ページ参照）も利用できます。

リモートストレージ同時接続：
現在、次の接続が可能です。

– 最大 **2** つまでのリモートストレージが、リモート管理端末の仮想ドライブとして接続できます（接続に、ビデオリダイレクション Java アプレットを利用した場合）。

あるいは

– **1** つのリモートストレージがリモートストレージサーバに接続できます。

アプレットを経由したリモートストレージ接続およびリモートストレージサーバは同時に利用できません。

「リモートストレージ」ページを使って、リモートストレージ接続の状況およびリモートストレージ接続の構成を行うことができます。

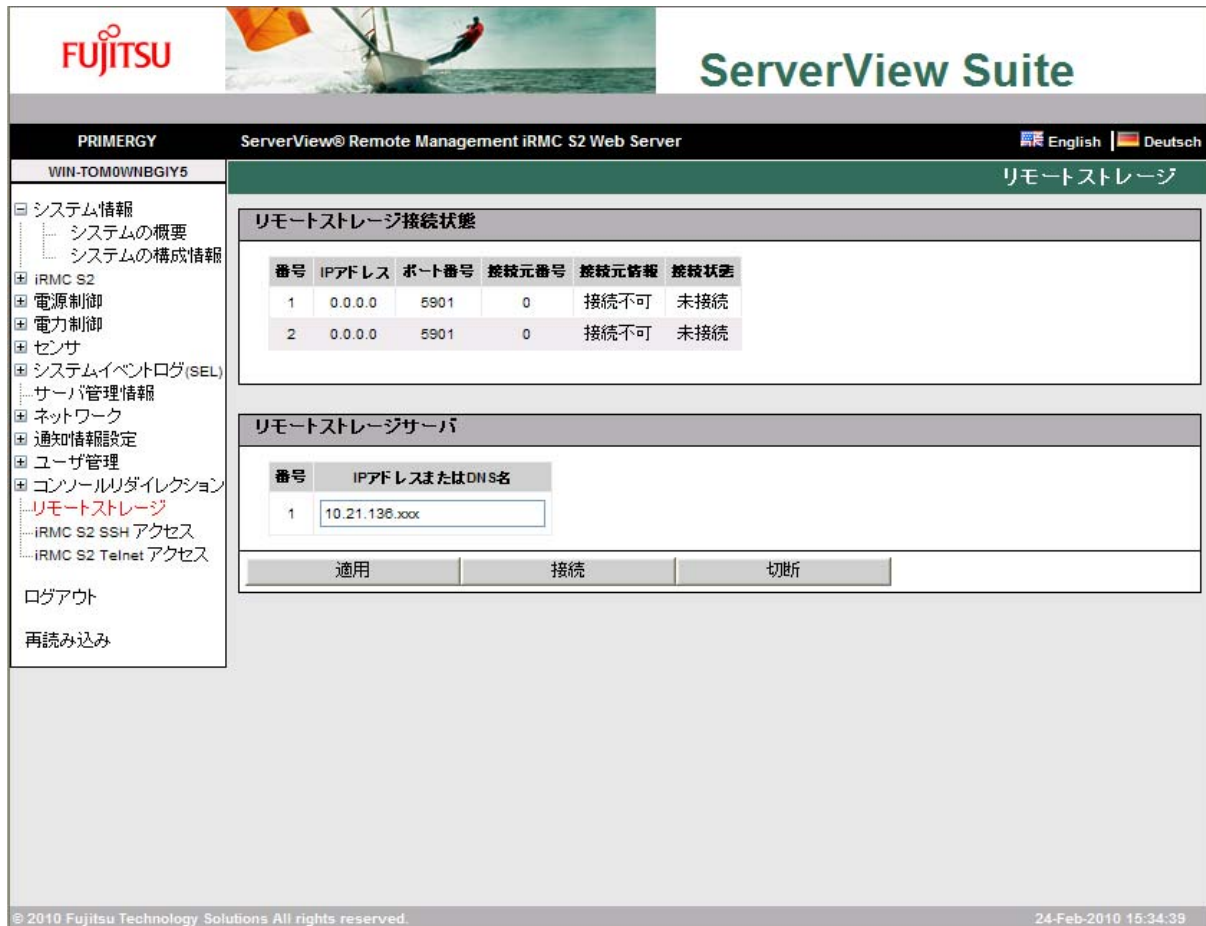



図 201 ：リモートストレージページ

「*IP アドレスまたは DNS 名*」

リモートストレージサーバがインストールされたコンピュータの IP アドレスあるいは DNS 名を入力してください。

［*適用*］

［接続］ボタンをクリックして、リモートストレージサーバの IP アドレスあるいは DNS 名を保存し、リモートストレージサーバとの接続を構成してください。

［接続］

［接続］ボタンをクリックして、リモートストレージサーバの IP アドレスあるいは DNS 名を保存し、リモートストレージサーバとの接続を構成してください。

i リモートストレージサーバとの接続を行う前に、リモートストレージサーバをインストールし、かつ、稼動させておかなければなりません。

［*切断*］

［切断］ボタンをクリックして、リモートストレージサーバとの接続を切断してください。

7.16 Telnet/SSH を経由した iRMC S2 の操作（Telnet/SSL での管理）

iRMC S2 では、Telnet/SSH ベースのインターフェースが可能です。これは、Telnet/SSL での管理と呼ばれています。Telnet/SSL での管理の英数字でのインターフェースを使って、システム、センサ、電力制御機能およびエラーイベントログにアクセスすることができます。テキストコンソールリのダイレクションおよび SMASH CLP シェルを開始することも可能です。

iRMC S2 Web インターフェースから、次の手順で、Telnet/SSL での管理を呼び出すことができます：

– 「*iRMC S2 SSH Access*」リンクを使って、SSH（セキュアなシェル）を初期化し、iRMC S2 に 暗号化された Telnet 接続を行うことができます。

– 「*iRMC S2 Telnet Access*」リンクを使って、iRMC S2 に、非暗号化 Telnet 接続を行うことができます。

i 並行接続の最大数：
－ Telnet： 最大 4 。
－ SSH： 最大 2 。
－ Telnet および SSH の合計： 最大 4 。

Telnet/SSL の管理を利用しての iRMC S2 の操作については、361 ページの「Telnet/SSH アクセス（Telnet/SSL での管理）」に記載されています。

管理サーバに関する要求

Telnet を経由した iRMC S2 へのアクセス（293 ページの「ポート番号とネットワークサービス－ポート番号とネットワークサービスの設定」の節参照）が、有効になっていなければなりません。

i パスワードがプレーンテキストで送信されるので、Telnet プロトコル経由でのアクセスは、初期設定では安全性の理由で無効になっています。

SSH/Telnet 接続の設定および Telnet/SSL での管理へのログイン

SSH および Telnet 接続の画面の違いは、各接続特有の情報が表示されるか否かです。SSH 接続の画面は下のように表示されます。

➢ ナビゲーションバーの「iRMC S2 SSH Access」（SSH）あるいは「iRMC S2 Telnet Access」（Telnet）のリンクをクリックしてください。

SSH あるいは Telnet 接続の Java アプレットが開始され、次の画面が表示されます（ここでは、SSH 接続の例を示します）：

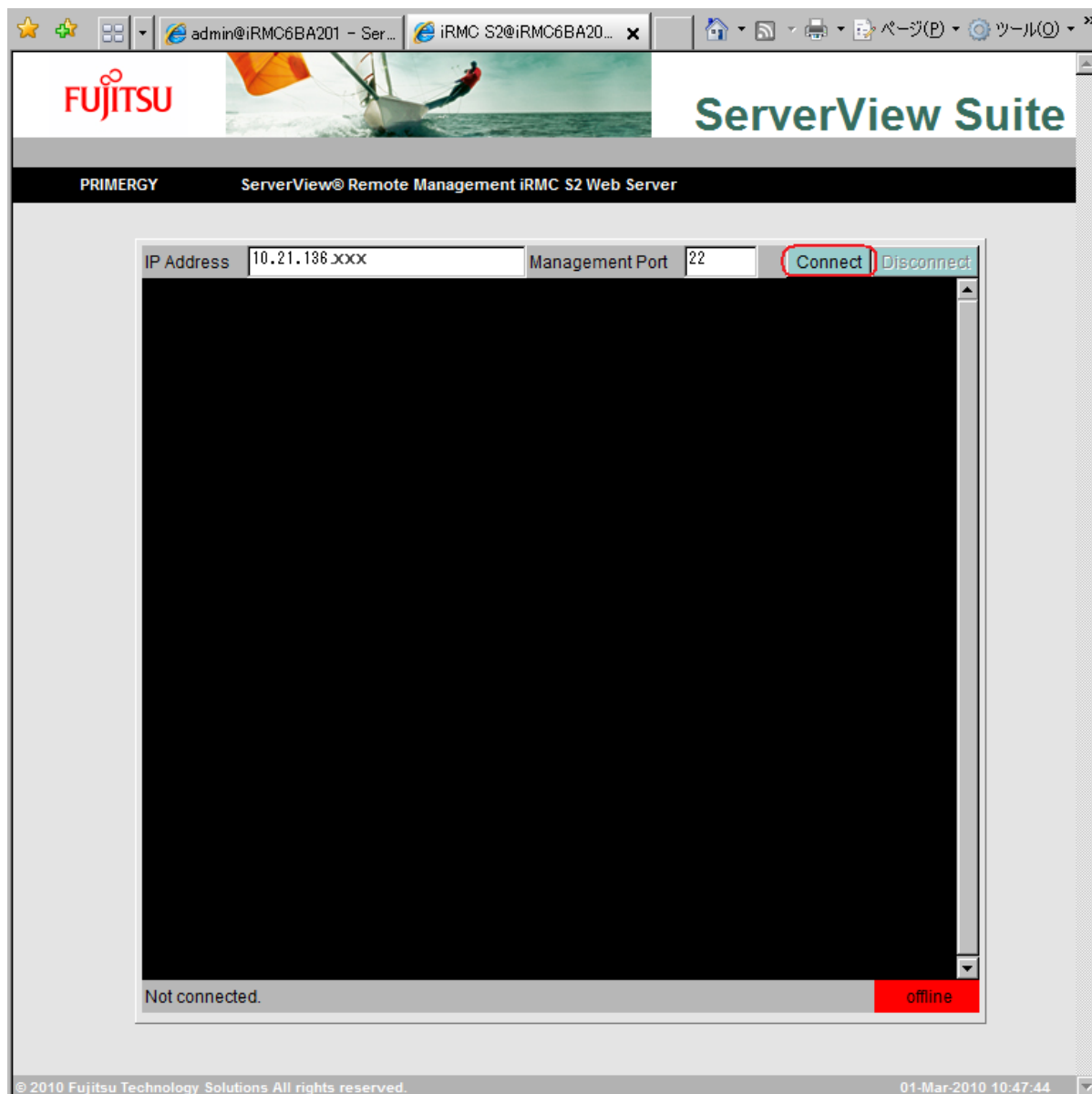



図 202 ： iRMC S2 への SSH 接続

➤ 接続バー内の［Connect］ボタンをクリックしてください。

iRMC S2 への接続が確立すると直ぐに、ユーザー名とパスワードの入力が要求されます。

－「*Logging into the Remote Manager over an SSH connection*」

i 管理サーバのホストキーがリモート管理端末に登録されていない場合、SSH クライアントに、ログインを続けるかについて、安全性の警告が表示されます。

次のログイン画面が表示されます。

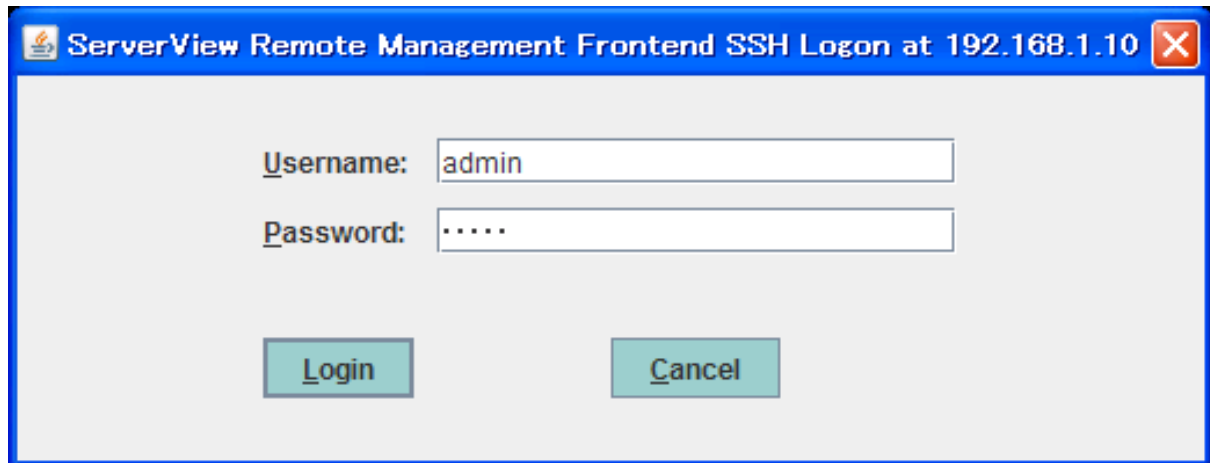



図 203：SSH 接続：Telnet/SSL での管理へのログイン

➤ ユーザー名とパスワードを入力して、［*Login*］ボタンをクリックして、入力を確定してください。

その後、Telnet/SSL での管理のメインメニューが表示されます（図 205 参照）。

– 「*Logging into the Remote Manager over an Telnet connection*」
次のログイン画面が表示されます。

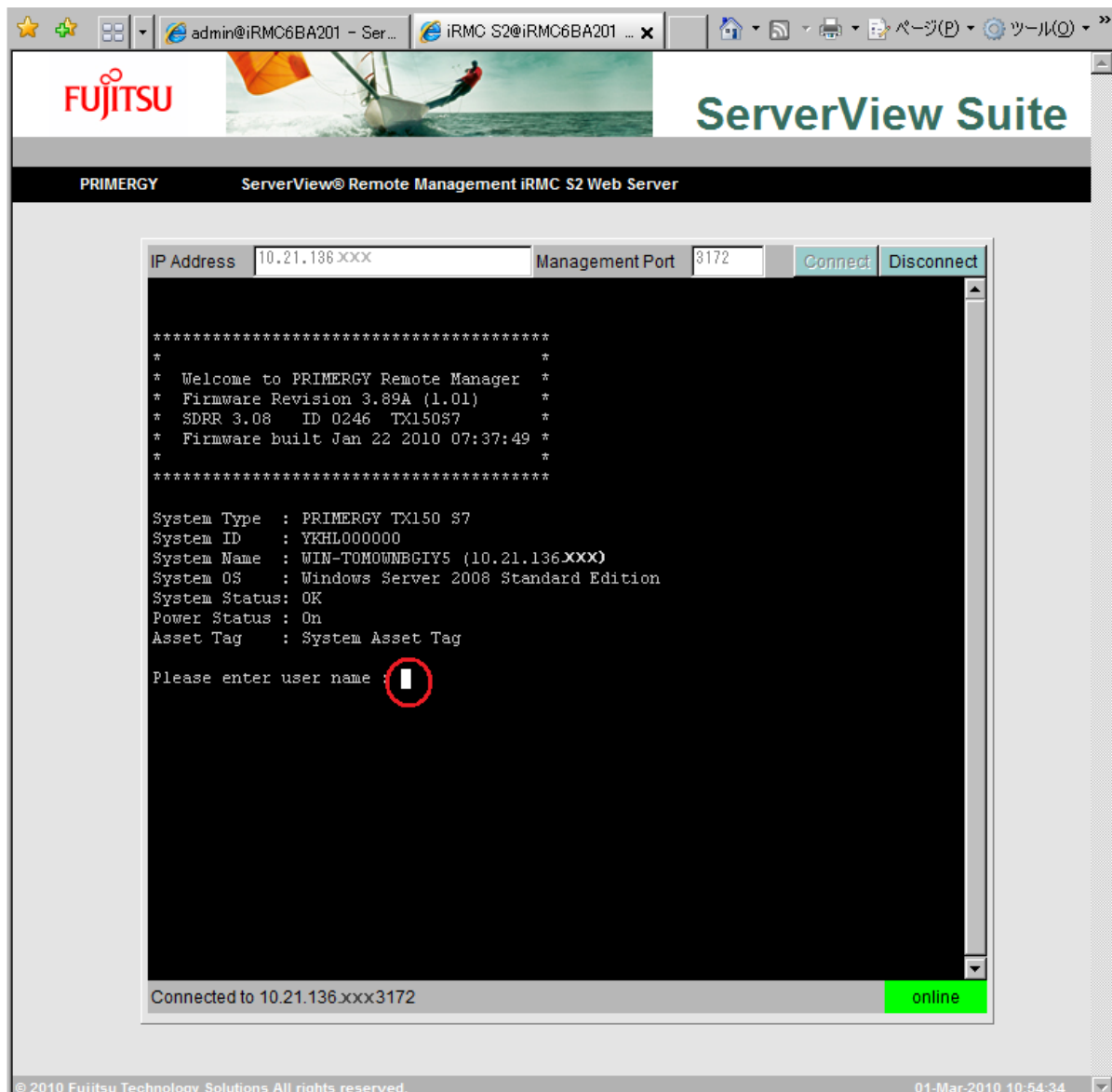



図 204 ： Telnet 接続：Telnet/SSL での管理へのログイン

ServerView エージェントがシステム上で稼動しているか否かにより、ログイン画面は、システム情報を表示あるいは非表示とします（366 ページ参照）。

➤ ユーザー名およびパスワードを入力し、[Enter] キーを押して、入力を確定してください。

その後、Telnet/SSL での管理のメインメニューが表示されます（図 205 参照）。

➤ 接続バー内の［Connect］ボタンをクリックしてください。

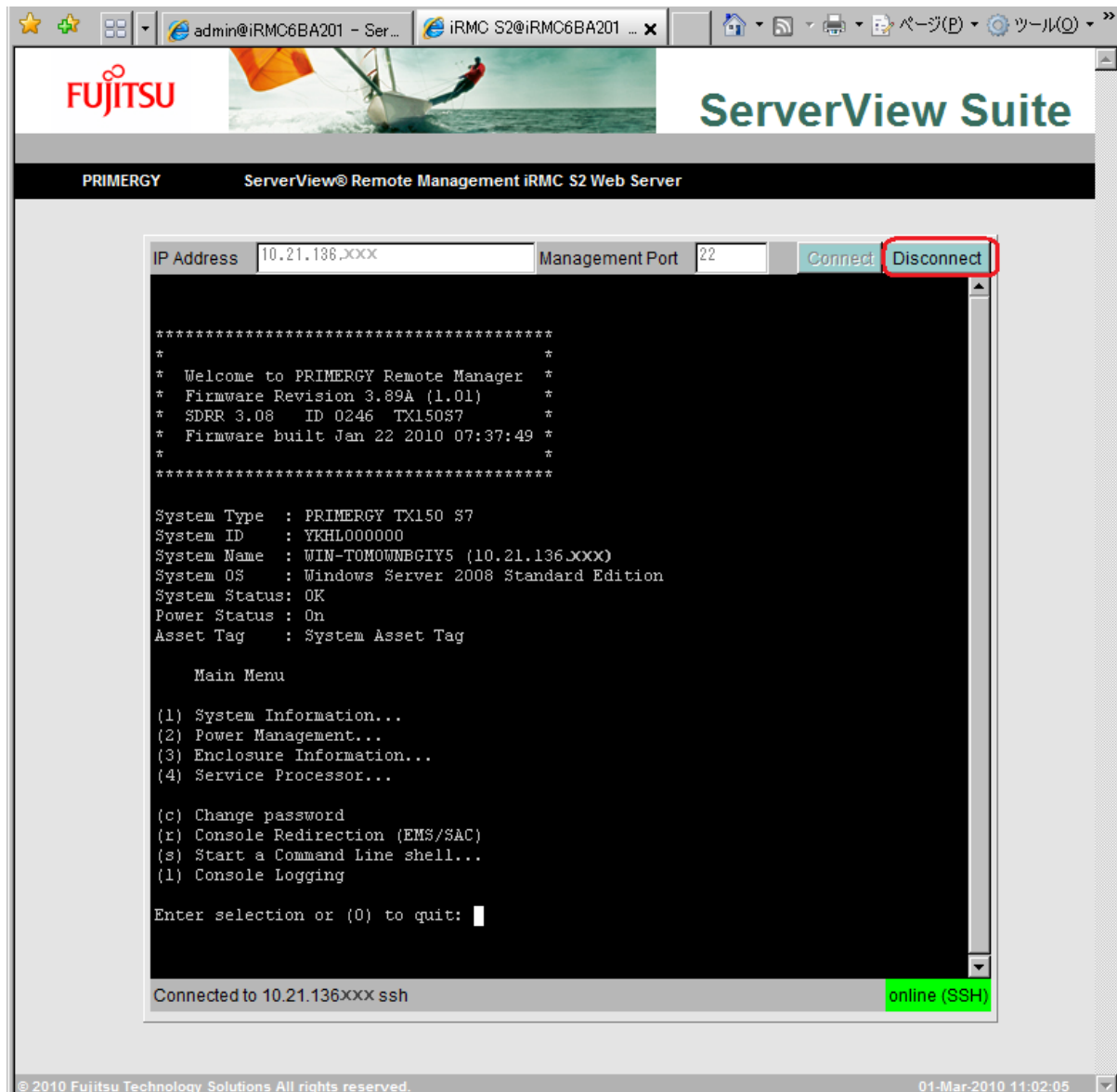



図 205 ：Telnet/SSL での管理メインメニュー

Telnet/SSH 接続の切断

➤ Telnet/SSL での管理への接続の切断は、Telnet/SSL での管理画面の接続バー内の［Disconnect］ボタン、あるいは、Telnet/SSL での管理画面へ 0 を入力することにより、可能です（図 205 参照）。

8 章 Telnet/SSH アクセス（Telnet/SSL での管理）

iRMC S2 には Telnet ベースのインターフェースも使用可能です。この方式が Telnet/SSL での管理です。Telnet/SSL での管理は以下のインターフェースから呼び出すことができます。

– iRMC S2 Web インターフェース（356 ページ参照）
– あらゆる Telnet/SSH クライアント
– ServerView リモートマネジメントフロントエンド

iRMC S2 は SSH（セキュアシェル）上のセキュリティ保護された接続をサポートします。Telnet/SSL での管理のインターフェースは Telnet および SSH 接続と同等です。
基本的には VT100 シーケンスを読みとれる Telnet/SSH クライアントであれば、iRMC S2 へのアクセスに使用できます。
ただし、iRMC S2 Web インターフェースまたは ServerView リモートマネジメントフロントエンド （略称をリモートマネジメントフロントエンドとします）のご使用を推奨します。

複数接続の最大数
– Telnet： 最大 4
– SSH： 最大 2
– Telnet と SSH 併用： 最大 4

管理対象サーバの必要条件

Telnet 経由の接続は、iRMC S2 用に有効化する必要があります。（293 ページ、「ポート番号とネット ワークサービス－ポート番号とネットワークサービスの設定」の節を参照してください。）

Telnet プロトコルによる接続は、パスワードが平文で転送されるため、初期設定ではセキュリティのために無効化されています。

ServerView Operations Manager は、管理ポートの値を知らないので、リモートマネジメントフロントエンドはデフォルト値で動作します。

リモートマネジメントフロントエンドは起動後、自動的には接続を開始しませんので、リモートマネジメントフロントエンド起動後に管理ポートの値を変更することができます。

8.1 ServerView リモートマネジメントフロントエンドによる iRMC S2 の運用

リモートマネジメントフロントエンドを使用した iRMC S2 接続の確立と、リモートマネジメントフロントエンドの作業環境に関する詳細な情報は、『ServerView Suite ServerView Remote Management Frontend』ユーザーガイドにあります。

8.2 Telnet/SSL での管理

本節では Telnet/SSL での管理による iRMC S2 の操作とさまざまな機能の詳細について説明します。本節の末尾には SMASH CLP の概略の説明もあります。

8.2.1 Telnet/SSL での管理の運用

リモートビューの操作は 図 206 の例に基づいて説明します。その図では Telnet/SSL での管理のメインメニューの一例が紹介されています。

```
    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password
(r) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging

Enter selection or (0) to quit: _
```

図 206 : Telnet/SSL での管理の操作

- メニュー項目から必要な番号または文字を入力して使用する項目を選択します。文字はメニュー項目の頭文字となっています。例えば「c」は「パスワードの変更」に対応します。

  ユーザーに使用が禁止されている機能はダッシュ (-) が付けられ、使用できない機能にはアスタリスク (*) が付けられます。

- ［0］キーを押下するか、［Ctrl］と［D］を同時に押下すると、Telnet/SSL での管理が終了します。関連するイベントはイベントログに記録されます。

8.2.2 メニューの概要

iRMC S2 Telnet/SSL での管理のメニューは以下の構造となっています。

- **System Information**
  - Chassis Information
  - Mainboard Information
  - OS and SNMP Information

- **Power Management**
  - Immediate Power Off
  - Immediate Reset
  - Power Cycle
  - Power on
  - Graceful Power Off (Shutdown)
  - Graceful Reset (Reboot)

- **Enclosure Information**
  - System Event-Log
    - View System Event-Log (text, newest first)
    - View System Event-Log (text, oldest first)
    - Dump System Event-Log (raw, newest first)
    - Dump System Event-Log (raw, oldest first)
    - View System Eventlog Information
    - Clear System Event-Log
  - Temperature
  - Voltages/Current
  - Fans
  - Power Supplies
  - Door Lock
  - CPU Sensors
  - Component Status (Lightpath)
  - List All Sensors

- **Service Processor**
  - Configure IP Parameters
  - List IP Parameters
  - Toggle Identify LED
  - Reset iRMC S2 (Warm reset)
  - Reset iRMC S2 (Cold reset)

- **Change password**
- **Console Redirection (EMS/SAC)**
- **Start a Command Line shell**
- **Console Logging**

8.2.3 ログイン

iRMC S2 への接続が確立されると、リモート管理端末のターミナルクライアント機に Telnet/SSL での管理のログインウィンドウ（Telnet/SSH ウィンドウ）が立ち上がります。

ServerView エージェントがシステム全体の中でいずれかのポイントで起動済みであるかによって、ログインウィンドウにはシステム情報が表示される場合とされない場合があります。

i SSH 接続によるログイン：管理対象サーバのホスト鍵がリモート管理端末にまだ登録されていない場合には、SSH クライアントはセキュリティ警告を発信し、合わせて登録方法を案内します。

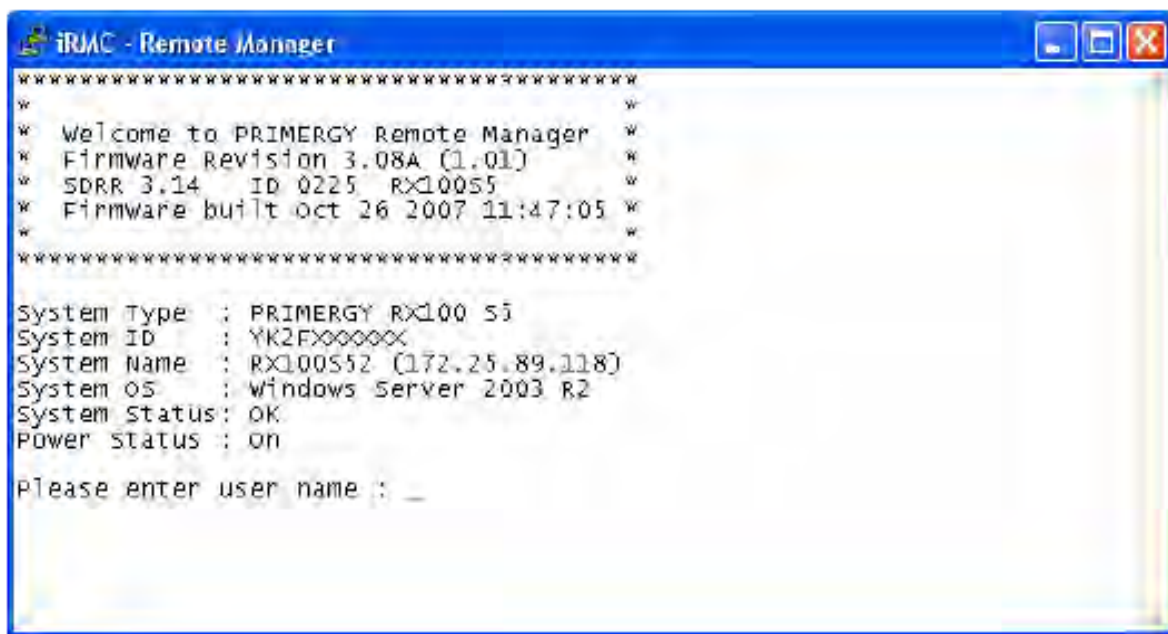



図 207：Telnet/SSL での管理 ログインウィンドウ（システム情報表示付き）

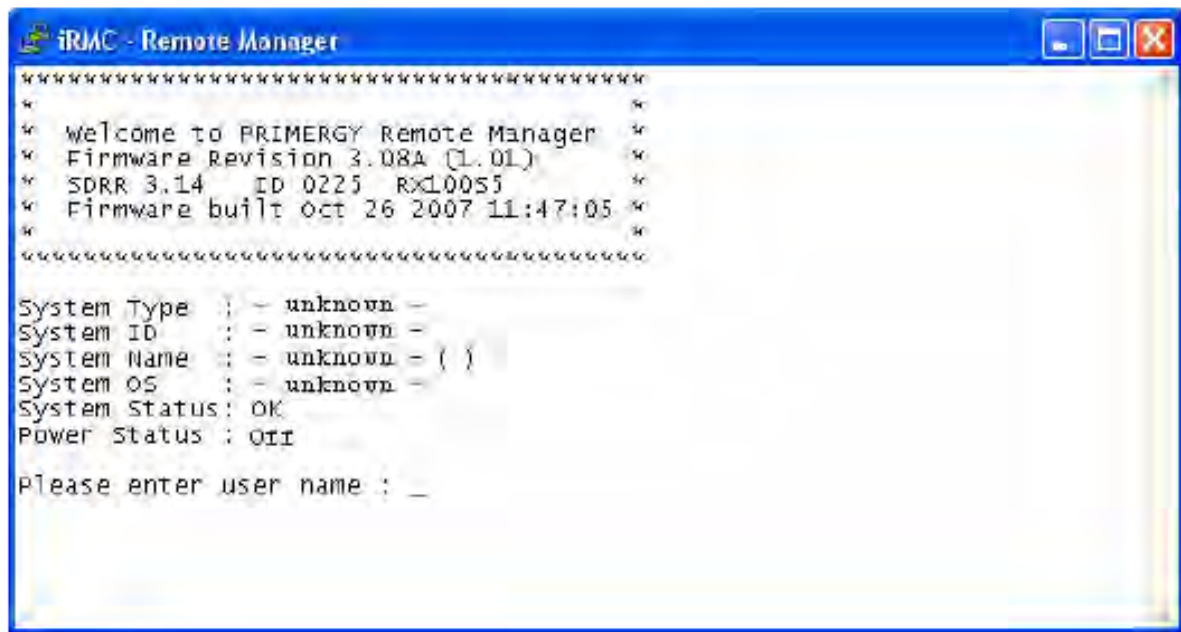



図 208： Telnet/SSL での管理 ログインウィンドウ（システム情報表示なし）

Telnet/SSL での管理ウィンドウには関連がある PRIMERGY システムの情報が表示されます。 この情報によりサーバが識別され、その運用状況（電源の状態）が表示されます。サーバの設定が適切である場合に限り、サーバに関する最小限の情報（たとえばシステム名）が表示されます。

➤Telnet/SSL での管理を使用可能とするためには、ユーザー名とパスワードを使用してログインしなければなりません。

関連するイベントがイベントログに書き込まれ、Telnet/SSL での管理のメインメニューが表示されます。（368 ページ、「Telnet/SSL での管理のメインメニュー」の節を参照してください。）

[Ctrl] + [D] を押下すればいつでもログイン処理を中止できます。

8.2.4 Telnet/SSL での管理のメインメニュー

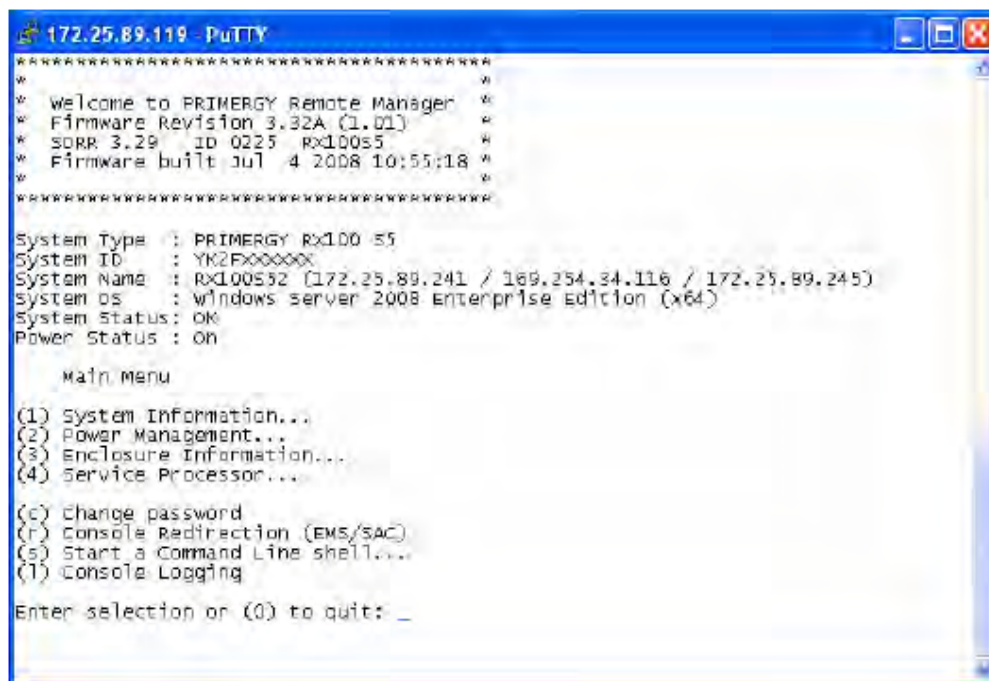



図 209：Telnet/SSL での管理： メインメニューウィンドウ

Telnet/SSL での管理のメインメニューには以下の機能があります。

「*System Information...*」	管理対象サーバの情報を表示します （372 ページ、「システム情報 - 管理対象サーバの情報」の節を参照してください。）
「*Power Management...*」	サーバの電源をオン / オフします。 （373 ページ、「Power Management」の節を参照して ください。）

表 9：Telnet/SSL での管理のメインメニュー

「*Enclosure Information...*」	現在のシステムの状態に関する情報を要求します。たとえば、エラーログやイベントトログ（温度、ファンの状態 など）からのエラーやイベントの情報を確認します。（375 ページ、「Enclosure Information - システムイベン トログとセンサの状態」の節を参照してください。）
「*Service Processor...*」	iRMC S2 を設定します（たとえばファームウェアの更新や IP アドレスの変更)。(379 ページ、「サービスプロセ ッサ - IP パラメータ、診断用 LED、および、iRMC S2 の リセット」の節を参照してください。)
「*Change password*」	パスワードを変更します。(371 ページ、「パスワード変 更」の節を参照してください。)
「*Console Redirection (EMS/SAC)*」	テキストコンソールをリダイレクトします。(380 ペー ジ、「コンソールのリダイレクション（EMS/SAC) - テ キストコンソールのリダイレクションの起動」の節を参照してください。)
「*Start a Command Line shell...*」	コマンドラインシェルを起動します (381 ページ、「コマ ンドラインシェルの起動 ... - SMASH CLP シェルの起動」の節を参照してください。)
「*Console Logging*」	メッセージ出力をテキストコンソールにリダイレクトします。(382 ページ、「コンソールログ - テキストコンソ ール（シリアル接続）へのメッセージ出力のリダイレク ション。」の節を参照してください。)

表 9：Telnet/SSL での管理のメインメニュー

8.2.5 必要なユーザークセス許可

Telnet/SSL での管理の個々の機能を利用するために必要なユーザークセス許可の概略を 表 10 に示し ます

表 10： Telnet/SSL での管理メニュー使用のアクセス許可

8.2.6 パスワード変更

特権がある「*Configure User Accounts*」（56 ページ参照）を持つユーザーは、「*Change password*」メニューの項目を使用して、自分のパスワードまたは他のユーザーのパスワードを変更することができます。

8.2.7 システム情報 - 管理対象サーバの情報

メインメニューから「*System Information...*」を選択すると以下のメニューが表示されます。

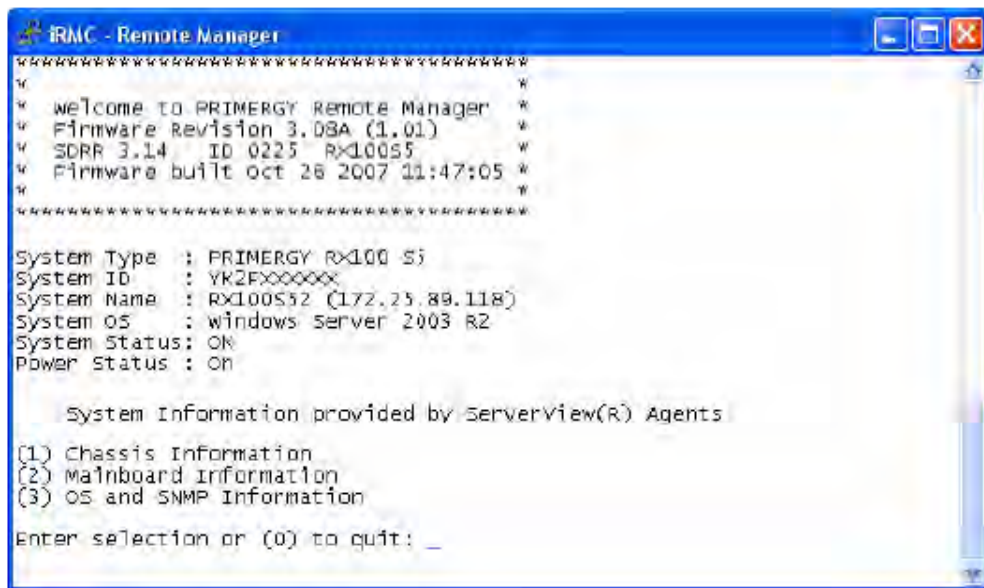



図 210： Telnet/SSL での管理： システム情報ウィンドウ

サブメニューには以下の機能があります。

「*Chassis Information*」	管理対象サーバのシャーシ情報と製品データ。
「*Mainboard Information*」	管理対象サーバのメインボード情報と製品データ。
「*OS and SNMP Information*」	管理対象サーバのオペレーティングシステムおよび ServerView のバージョンと SNMP 設定の情報。

表 11： システム情報メニュー

8.2.8 Power Management

メインメニューから「*Power Management...*」を選択すると以下のメニューが表示されます。

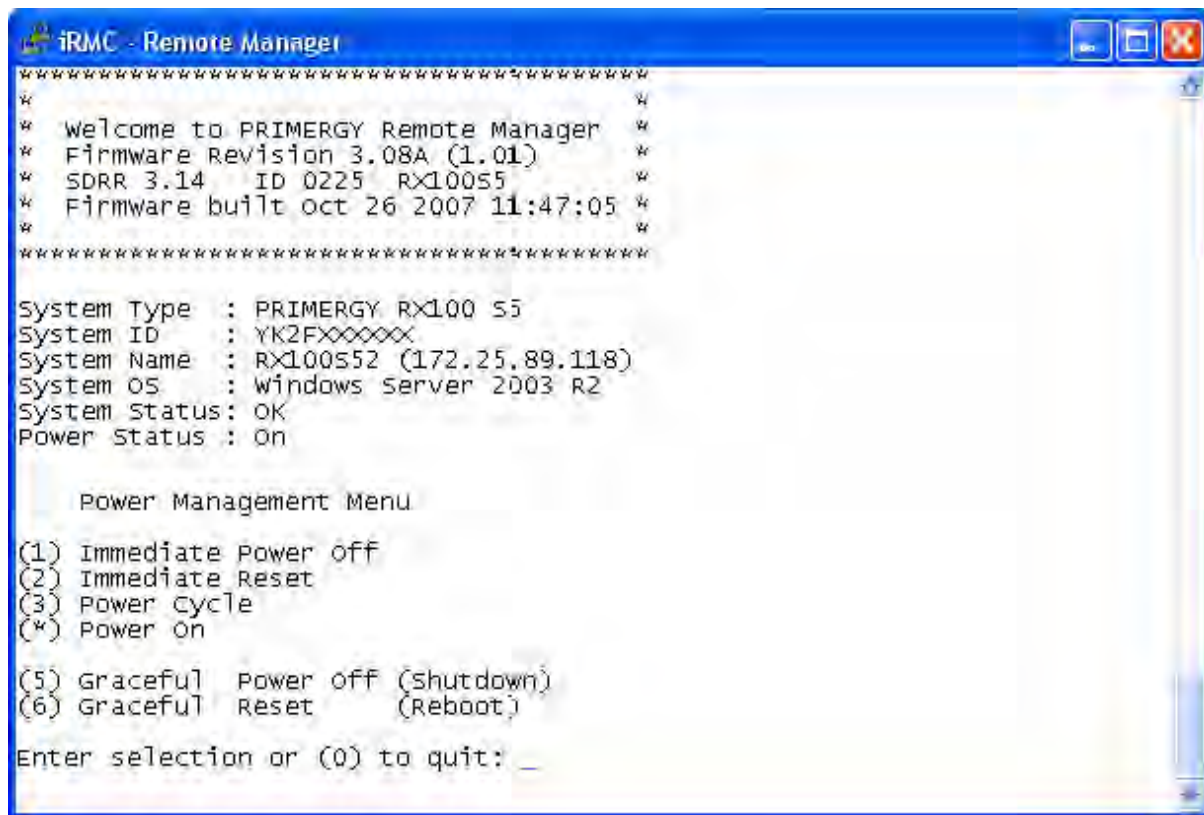



図 211： Telnet/SSL での管理： Power Managemaent ウィンドウ

このサブメニューには以下の機能があります。

「*Immediate Power Off* 」	サーバの電源を、オペレーティングシステムの状態に関係なく落とします。
「*Immediate Reset* 」	オペレーティングシステムの状態に関係なくサーバを完全に再起動させます（コールドスタート）。
「*Power Cycle* 」	サーバの電源を完全に落とした後、設定された時間をおいて立ち上げなおします。
「*Power On* 」	サーバをスイッチオンします。
「*Graceful Power Off (Shutdown)* 」	シャットダウン後に電源を落とします。このメニューは、ServerView エージェントがインストールされ、iRMC S2 に「Connected」とサインインされた場合のみ使用可能です。
「*Graceful Reset (Reboot)* 」	シャットダウン後にリブートします。このメニューは、ServerView エージェントがインストールされ、iRMC S2 に「Connected」とサインインされた場合のみ使用可能です。

表 12 :「Power Management」メニュー

8.2.9 Enclosure Information - システムイベントログとセンサの状態

メインメニューから「*Enclosure Information...*」を選択すると以下のメニューが表示されます。

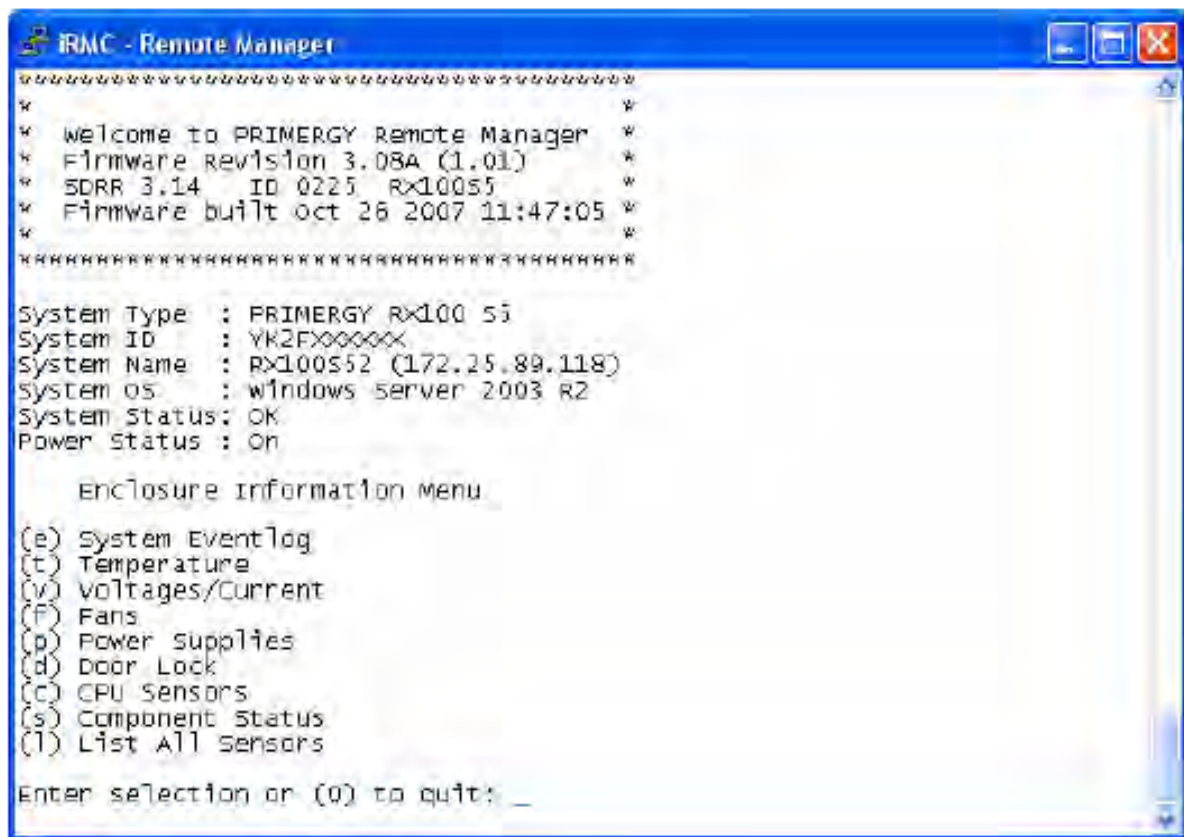



図 212： Telnet/SSL での管理： 「Enclosure Information」ウィンドウ

このサブメニューには以下の機能があります。

「*System Eventlog*」	システムイベントログメニューを呼び出します。(377 ページ、「システムイベントログ」の節参照。)
「*Temperature* 」	温度センサ情報とその状態を表示します。
「*Voltages/Current* 」	電圧/電流値の情報とその状態を表示します。
「*Fans* 」	冷却ファンの情報とその状態を表示します。
「*Power Supplies* 」	電源装置の情報とその状態を表示します。
「*Door Lock* 」	前面パネルまたはハウジングが開いていないかを表示します。
「*CPU Sensors* 」	サーバのプロセッサを適合させます。
「*Component Status* 」	PRIMERGY 診断 LED を備えたすべてのセンサの詳細情報を表示します。
「*List All Sensors* 」	すべてのセンサの詳細情報を表示します。

表 13 :「Enclosure Information」メニュー

システムイベントログ

「*Enclosure information...*」サブメニューから「*System Eventlog*」を選択すると以下のメニューが表示されます。

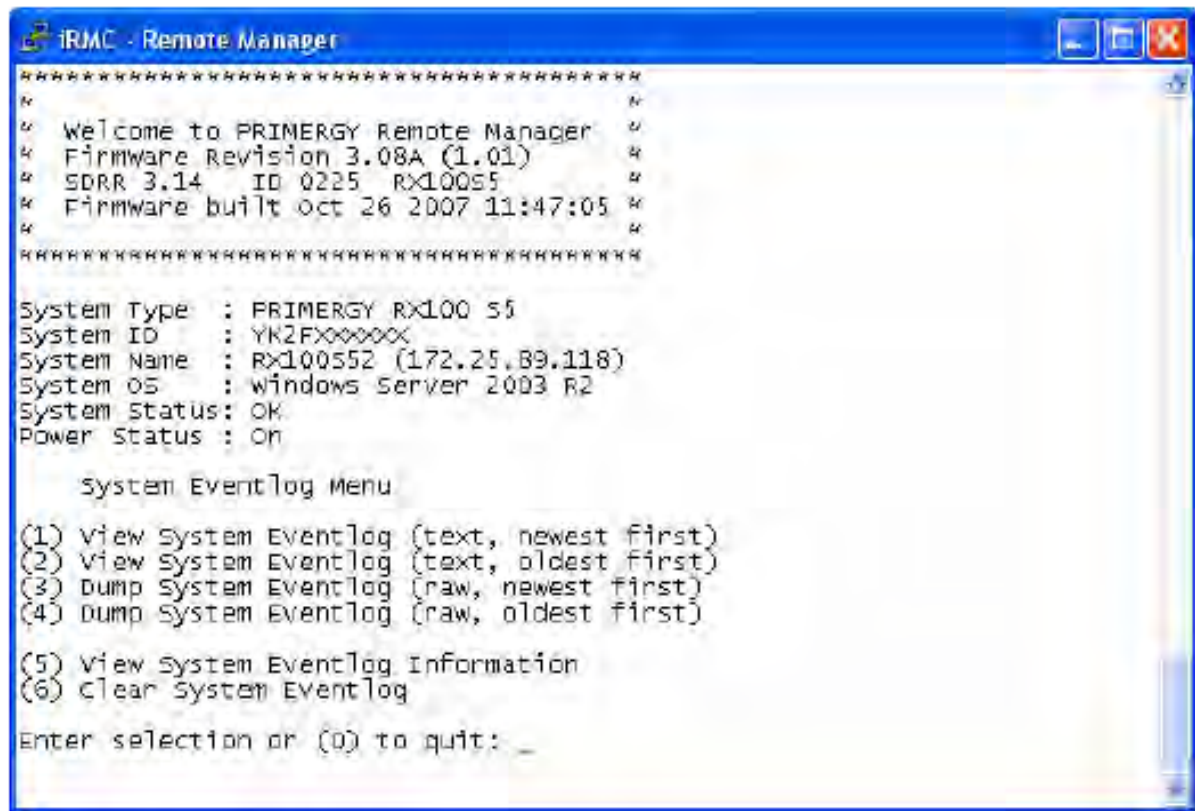



図 213： Telnet/SSL での管理： システムイベントログウィンドウ

このサブメニューには以下の機能があります。

「*View System Eventlog*」*(text, newest first)*	システムイベントログの内容が読み取れるフォーマットで時間順（最も新しいエントリが先頭）に画面に出力されます。
「*View System Eventlog*」*(text, oldest first)*	システムイベントログの内容が読み取れるフォーマットで逆時間順（最も古いエントリが先頭）に画面に出力されます。
「*Dump System Eventlog*」*(raw, newest first)*	イベントログの内容が時間順に（最も新しいエントリが先頭）ダンプされます。
「*Dump System Eventlog*」*(raw, oldest first)*	イベントログの内容が逆時間順に（最も古いエントリが先頭）ダンプされます。
「*View System Eventlog*」*Information*	イベントログに関する情報を表示します。
「*Clear System Eventlog*」	イベントログの内容をすべて消去します。

表 14： システムイベントログメニュー

8.2.10 サービスプロセッサ - IP パラメータ、診断用 LED、および、iRMC S2 のリセット

メインメニューから「*Service Processor...*」を選択すると以下のメニューが表示されます。

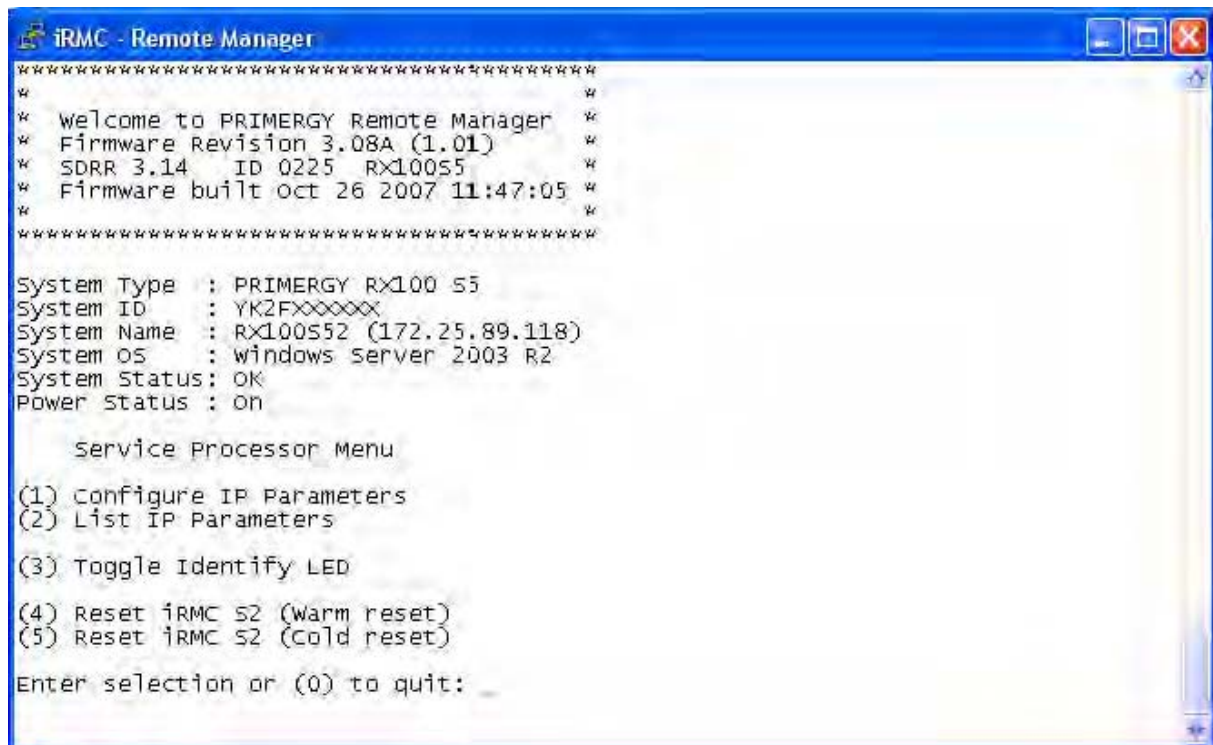



図 214： Telnet/SSL での管理： サービスプロセッサウィンドウ

このサブメニューには以下の機能があります。

「*Configure IP Parameters* 」	IP アドレスの設定、サブネットマスクとデフォルトゲートウェイ。DHCP を有効にするかどうかも指定できます。
「*List IP Parameters* 」	IP の設定を表示します。
「*Toggle Identify LED* 」	PRIMERGY の識別灯 のオン／オフを切り換えます。
「*Reset iRMC S2* 」*(warm reset)*	iRMC S2 をリセットします。接続が閉じられます。インターフェースのみが再起動されます。
「*Reset iRMC S2* 」*(cold reset)*	iRMC S2 をリセットします。接続が閉じられます。iRMC S2 全体が再起動します。

表 15 : サービスプロセッサ

i *iRMC S2* をコールドリセットまたはハードリセットでリセットした後にサーバをリブートすることを推奨します。(253 ページを参照してください。

8.2.11 コンソールのリダイレクション（EMS/SAC）テキストコンソールリダイレクションの起動

メインメニューから、「*Console Redirection (EMS/SAC)*」の項目によりコンソールのリダイレクションを起動させることができます。

i テキストベースのコンソールリダイレクションはシリアル 1 の LAN 上のみで機能します。テキストベースのコンソールリダイレクションは、英数字専用です。

コンソールのリダイレクションをオペレーティングシステムの稼働中に使用する場合は、シリアル *1* のマルチプレクサはシステム側に設定してください。

i 「<ESC>(」（または「~（チルダー）」）のキーボードショートカットを使用してテキストコンソールを終了させてください。

使用する PRIMERGY サーバのタイプによっては、これらのオプションのうちひとつしか使えない場合もあります。

8.2.12 コマンドラインシェルの起動 ... - SMASH CLP シェルの起動

メインメニューの「*Command Line shell...*」コマンドラインシェルの起動を使用して、「SMASH CLP」シェルを起動させることができます。SMASH CLP は「Systems Management Architecture for Server Hardware Command Line Protocol」の各々の頭文字をとったものです。このプロトコルにより、管理用端末と管理対象サーバの間で Telnet または SSH をベースとした接続が可能となります。SMASH CLP のより詳しい情報は、385 ページの「コマンドラインプロトコル（CLP)」の節を参照してください。

メインメニューから「(s) Start a Command Line shell...」コマンドラインシェルの起動 ... を選択すると、以下のウィンドウが立ち上がります。

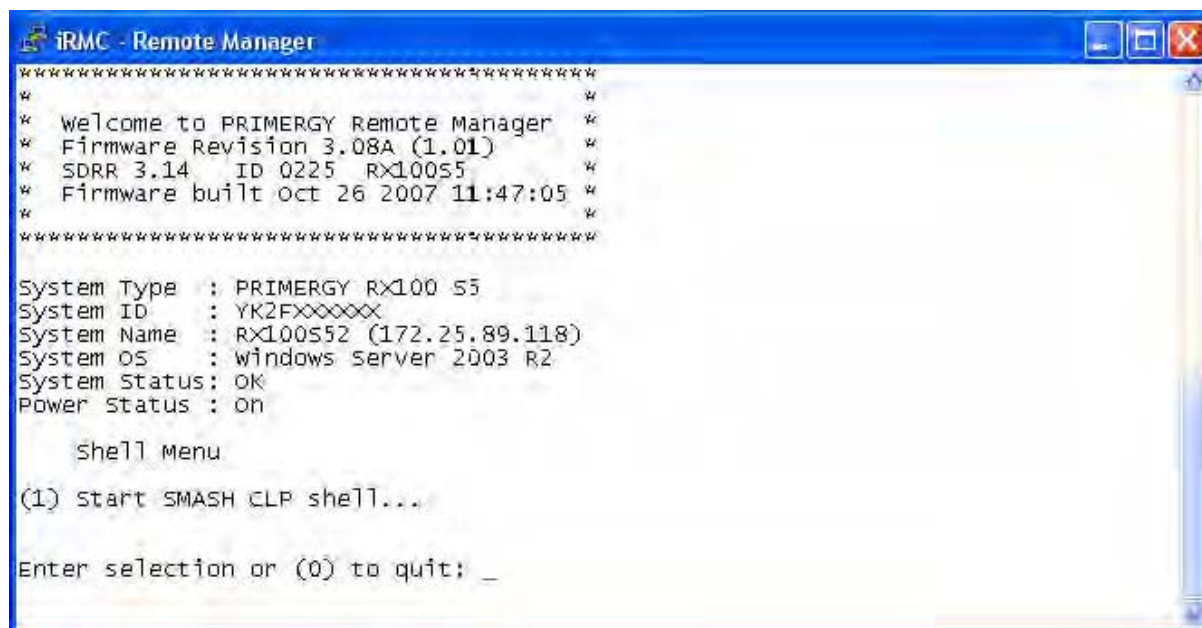



図 215： Telnet/SSL での管理： SMASH CLP シェルの起動 ... ウィンドウ

➤「Start a SMASH CLP shell ...」を選択して SMASH CLP shell を起動してください。

8.2.13 コンソールログ - テキストコンソール（シリアル接続）へのメッセージ 出力のリダイレクション

メインメニューの「*Console Logging*」により、メッセージ出力（ログ）をテキストコンソール（シリアルインターフェース）にリダイレクトすることができます。

メインメニューから「*(l) Console Logging*」を選択すると以下のウィンドウが表示されます。

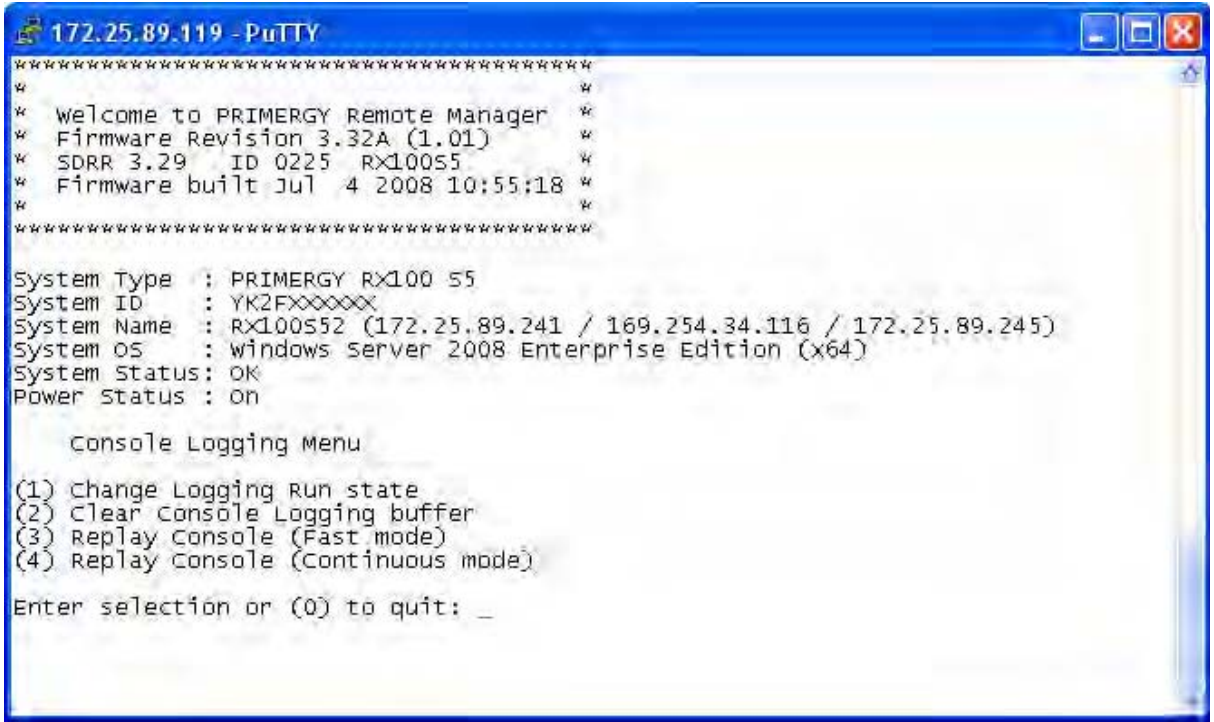



図 216： Telnet/SSL での管理： コンソールのログ

このサブメニューには以下の機能があります。

「**Change Logging Run State**」	ログ実行状態の表示と変更。より詳しい説明は、383 ページの「コンソールログ実行状態メニュー」を参照してください。
「**Clear Console Logging Buffer**」	コンソールログバッファを消去します。
「***Replay Console (Fast mode)***」	コンソールログを表示します（高速モードで）
「***Replay Console (Continuous mode)***」	コンソールログを表示します （連続モードで）

表 16： コンソールログメニュー

コンソールログ実行状態メニュー

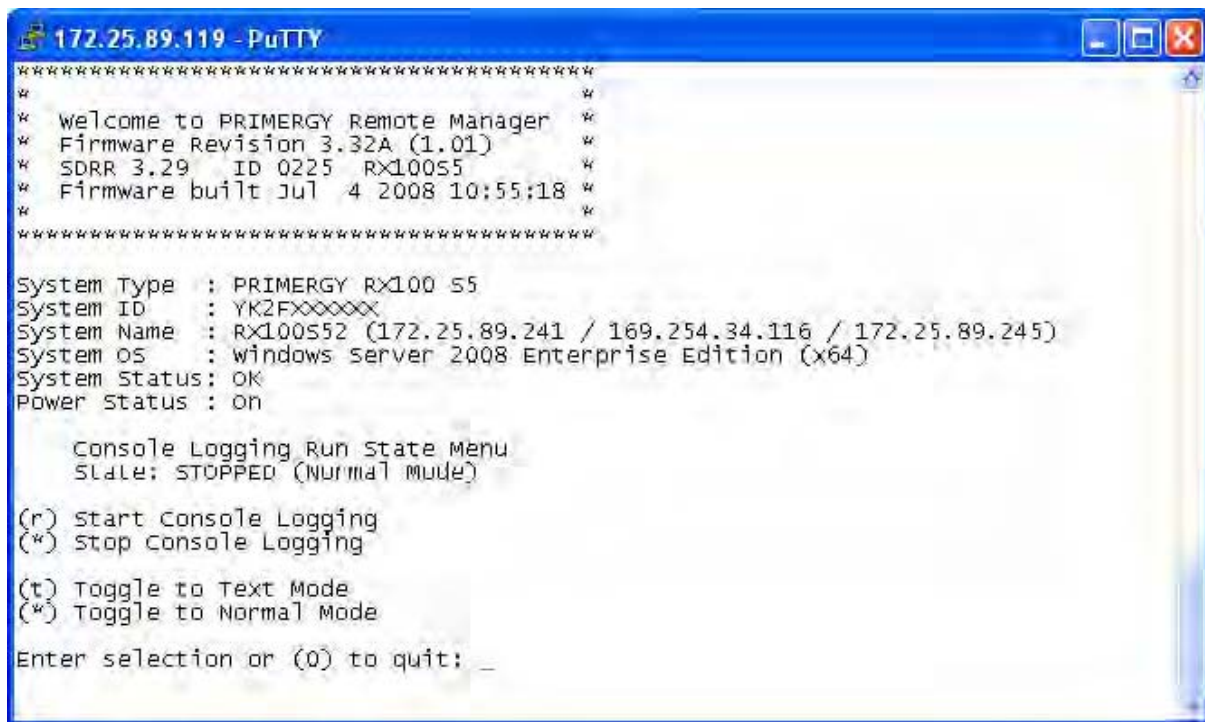



図 217 : Telnet/SSL での管理 : コンソールログ実行状態メニュー

「*Console Logging Run State Menu*」コンソールログ実行状態メニューには以下の機能があります。

「*Start Console Logging*」	テキストコンソールへのメッセージ出力開始。
「*Stop Console Logging*」	テキストコンソールへのメッセージ出力を中止します。
「*Toggle to Text Mode*」	テキストモードに切り替えます。メッセージをコンソールに出力する前に、エスケープシーケンスをすべてフィルタにかけます。
「*Toggle to Normal Mode*」	ノーマルモードに切り替えます。ノーマルモードでは、メッセージをコンソールに出力する前に、以下のエスケープシーケンスをフィルタにかけます。 <ESC>（ <ESC>stop <ESC>Q <ESC>R<ESC>r<ESC>R <ESC>^ すなわち、カラー、疑似グラフィックスなどは限られた範囲内で再現させることができます。

表 17： コンソールログ実行状態メニュー

8.2.14 コマンドラインプロトコル（CLP）

iRMC S2 はユーザーシェルとも呼ばれるさまざまなテキストベースのユーザーインターフェースをサポートします。個々のユーザーが別々に設定することができます。

System Management Architecture for Server Hardware (SMASH) 協議会は以下の目的でさまざまな規格を規定しました。

– 異種コンピュータ環境を管理する標準化インターフェースの規定、

– 統一インターフェース、ハードウェアとソフトウェアの検出、リソースアドレス割り当て、および、データモデルなどのアーキテクチャフレームワークの規定。

SMASH に関する詳しい説明は下記のリンクから得ることができます。

http://www.dmtf.org/standards/smash

SMASH CLP 構文

SMASH CLP は、インターネットによるコンピュータ管理や、企業やプロバイダー環境ための共通コマンドライン構文とメッセージプロトコルセマンティックを定めます。SMASH CLP の詳細な情報は、DMTF の文書『Server Management Command Line Protocol Specification (SM CLP) DSP0214』から得られます。

CLP の基本的な構文は以下の通りです。
<verb> [<options>] [<target>] [<properties>]

<verb>

Verb はコマンドまたは実行するアクションを指定します。verb のリストではたとえば以下のアクションを記述しています。

– データの確立（*set*）と取得（*show*）、

– ターゲットのステータス変更（*reset*、*start*、*stop*）、

– 現行のセッションの管理（*cd*、*version*、*exit*）、

– コマンドの説明を返す（*help*）

iRMC S2 システムでは、*oemfujitsu* という verb によって特殊な OEM コマンドを使用できます。

<option>

option コマンドは、verb のアクションまたは振舞いを変更します。Option はコマンドライン中で verb のすぐ後ろに置くことができ、必ずダッシュ（「-」）でつなぎます。たとえば、option は以下のように使用します。
– 出力フォーマットを規定する、
– コマンドを再帰的に実行させる、
– コマンドのバージョンを表示させる、あるいは
– Help を呼び出す。

<target>

<target> はコマンドが取り扱うオブジェクト、すなわち、コマンドのターゲットのアドレスまたはパスを指定します。ターゲットは単一の管理要素とすることができます。たとえば、ハードディスク、ネットワークアダプタ（ネットワークインターフェースカード、NIC）、もしくは、管理プログラム（Management Assistance Program、MAP）そのものでも可能です。ターゲットはトランスポートサービスなどのサービスとすることもできます。

たとえば、全体のシステムなど、管理プログラムによって管理できる複数の項目でもひとつの <target> で包括することもできます。

それぞれのコマンドに指定できる <target> はひとつのみです。

<properties>

<properties>は、コマンドの実行に必要なコマンドのターゲットのプロパティを記述します。すなわち、<properties> はコマンドにより取得または変更されるターゲットのクラスを識別します。

CLP 中のユーザーデータ構成（概要）

CLP の中のデータは階層構造になっています。「*cd*」コマンドを使用してこのストラクチャの中で移動することができます。

CLP の中のユーザーデータ構成の概要は 図 218 にあります。各ボックス中の名前がコマンドのターゲットを示します。 階層の各レベルに記されたコマンド /verb は使用可能な target、properties、および、verb を表しています。

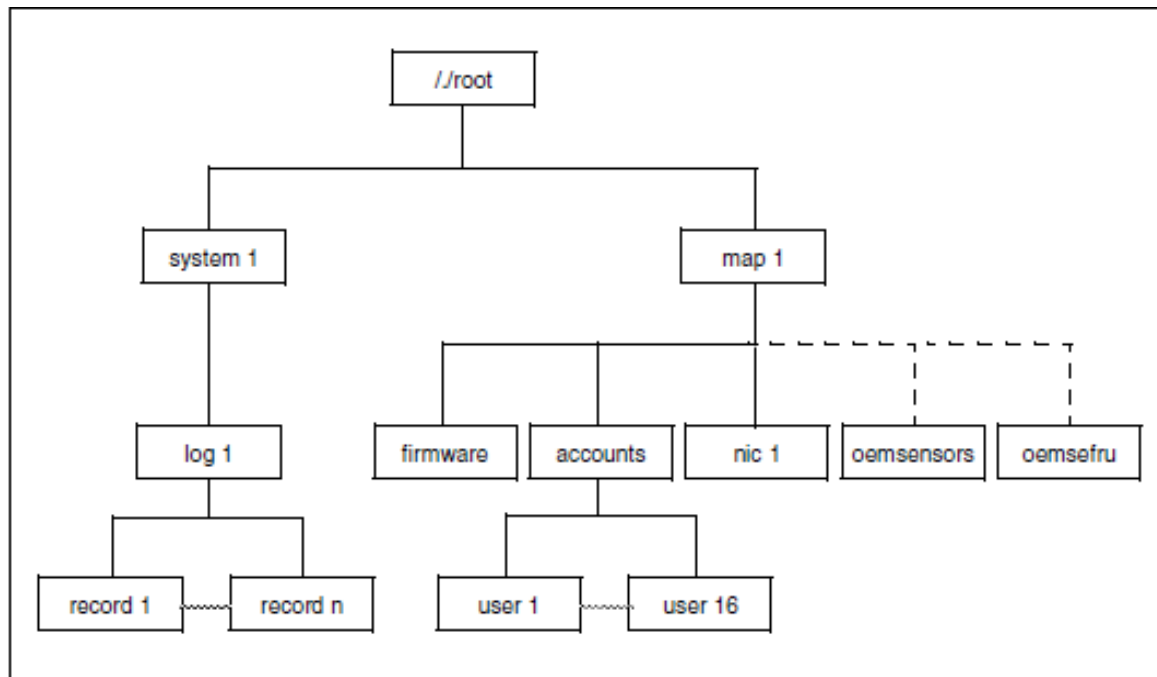



図 218： SMASH CLP のユーザーデータのストラクチャ

CLP コマンドの階層

CLP コマンド階層の概要は、388 ページの表 18 にあります。

Target \ Verb	Properties	Comment	cd	show	help	exit	version	set	reset	start	stop	load	oemfsc
// **system1** **map1**		Root	X	X	X	X	X						
system1	name enabledstate	Host System	X	X	X	X	X		System	PON	POFF		
...log1		Event Log (SEL)	X	X	X	X	X		iRMC				X
....record<n>	number date time sensordescription eventdescription eventdirection	Single SEL entry	X	X	X	X	X		iRMC				X
map1	name	iRMC	X	X	X	X	X		iRMC				X
...firmware	version	iRMC FW	X	X	X	X	X		iRMC			X	X
...accounts		Accounts	X	X	X	X	X	X	iRMC				X
......user<n>	username password group	User	X	X	X	X	X	X	iRMC				X
...nic1	networkaddress oemfsc_nonvol_networkaddress oemfsc_mask oemfsc_nonvol_mask oemfsc_gateway oemfsc_nonvol_gateway oemfsc_dhcp_enable oemfsc_nonvol_dhcp_enable oemfsc_vsi_path oemfsc_vsi_server oemfsc_vsi_permission oemfsc_vsi_sustain	LAN	X	X	X	X	X	X	iRMC				X
...oemfsc_sensors		OEM Sensors	X	X	X	X	X		iRMC				X
.....oemfsc_sensor_num<n>lun<m>	oemfsc _reading oemfsc _status oemfsc _sensortype oemfsc _readingtype	Single Sensor	X	X	X	X	X		iRMC				X
...oemfsc_frus		FRU	X	X	X	X	X		iRMC				X
.....oemfsc_fru_devid<n>lun<m>	oemfsc _description	Single FRU	X	X	X	X	X		iRMC				X

表 18： CLP コマンドの階層

9 章 サーバの設定を使用した iRMC S2 設定

本章は、以下の目的で Server Configuration Manager を使用する方法を説明します。

– iRMC S2 の設定（406 ページより）、

– iRMC S2 上のユーザー ID の設定と管理（421 ページより）

– iRMC S2 上のディレクトリサービスの設定（427 ページ参照）。

iRMC S2 は管理対象サーバによりローカルで設定することもでき、また、ServerView Operations Manager（以降 Operations Manager と略します）経由でリモート管理端末から設定することもできます。

要件：
管理するサーバには最新の ServerView エージェントをインストールしておく必要があります。

Server Configuration Manager の機能には以下の方法でアクセスすることができます。

– ローカルで管理対象サーバから「ServerStart」を使用

– ローカルで Windows 機の管理対象サーバから「Windows Start」メニューを使用

この方法がサポートされるのは、Windows 用の ServerView エージェントがインストールされたサーバのみです。

– リモートで Operations Manager のグラフィカルインターフェースを使用

この方法がサポートされるのは、Windows 用の ServerView エージェントがインストールされたサーバのみです。

9.1 System Configuration の起動

本節では、Server Configuration Manager、ウィンドウズスタートメニュー、および、ServerView Operations Manager を呼び出す方法を解説します。

各々の Server Configuration Manager のユーザーインターフェースはレイアウトの面で多少の違いはありますが、機能的には同一です。

Operations Manager から呼び出される Server Configuration Manager のダイアログボックスは、iRMC S2 の設定に使用する Server Configuration Manager のダイアログボックスの解説の中で触れることとします（406 ページ以降参照）。

9.1.1 Server Configuration Manager の ServerView Installation Manager からの呼び出し

Server Configuration Manager は、ServerView Installation Manager（以降、Installation Manager と略します）からも呼び出すことができます。Installation Manager 経由の設定は、サーバのインストール時に重要になります。Installation Manager は Server Configuration Manager を、インストールの準備中であっても、別のメンテナンスプログラムとしても、どちらでも使用可能にします。Installation Manager は『ServerView Suite ServerView Installation Manager』ユーザーガイドの中で詳しく説明されています。

9.1.2 Server Configuration Manager のウィンドウズスタートメニ ューからの呼び出し

Windows 機のサーバでは、Windows スタートメニューから Server Configuration Manager を呼び出すこともできます。

この作業は以下のように行います。

➤ 管理対象サーバ上で以下のように選択します。

「スタート」→「すべてのプログラム」→「*Fujitsu ServerView Suite*」→「*Agents*」→「*Configuration Tools*」→「*System Configuration*」

「*System Configuration*」ウィンドウが開きます。

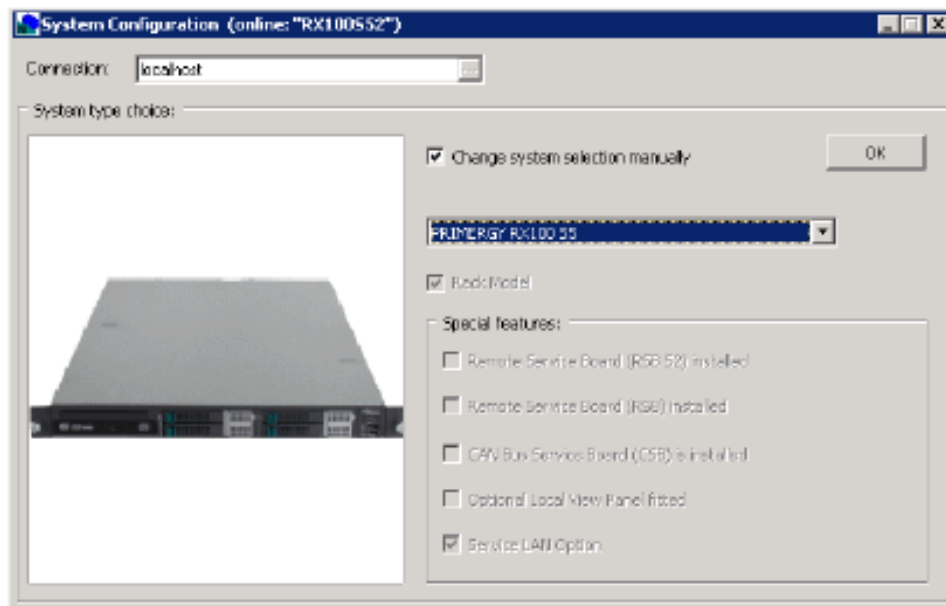



図 219 :「System Configuration」ウィンドウ

➤ 設定済みの値を承認します。

➤［*OK*］をクリックします。

「*System Configuration*」ウィンドウのタブビューが開きます。

タブの横にある矢印をクリックして、タブを左または右にスクロールすることができます。

設定の適用

各タブで以下の通り進めて、個々のタブで行った設定を適用してください。

➢［*Apply*］ボタンをクリックしてください。

➢［*Save Page*］ボタンをクリックします。

iRMC S2 は自動的にリブートされ設定の変更が有効化されます。

9.1.3 Server Configuration Manager の Operations Manager からの起動

iRMC S2 設定に使用する Server Configuration Manager のダイアログボックスは、Operations Manager のグラフィカルユーザーインターフェースからも使用できます。このため、リモート管理端末の管理対象サーバからも Web インターフェース経由で、iRMC S2 を設定することができます。

以下の通り進めます。

➢ Operations Manager を起動します。(『ServerView Suite Operations Manager』ユーザーガイドを参照してください。)

Operation Manager のスタートウィンドウが開きます。

図 220：Operation Manager： スタートウィンドウ

➢ Operation Manager のスタートウィンドウの「*管理者設定*」メニューから「サーバの設定」を選んでください。

その結果以下のウィンドウが開かれます：

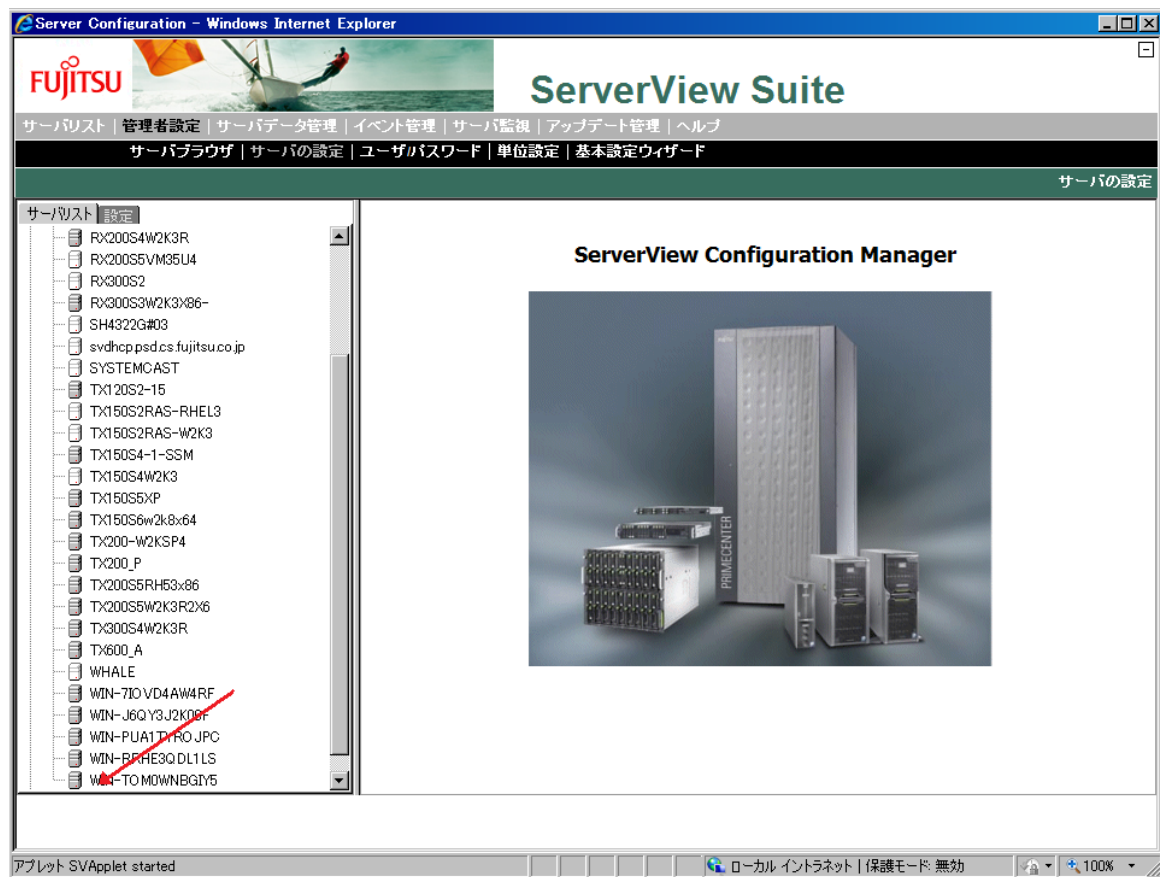



図 221：Operation Manager： サーバコンフィグレーションウィンドウ - 「サーバリスト」（1） タブ

➤「サーバリスト」タブの階層ツリーから、設定するサーバを選択してください。以下のウィンドウが開きます：（図 222 を参照してください。）

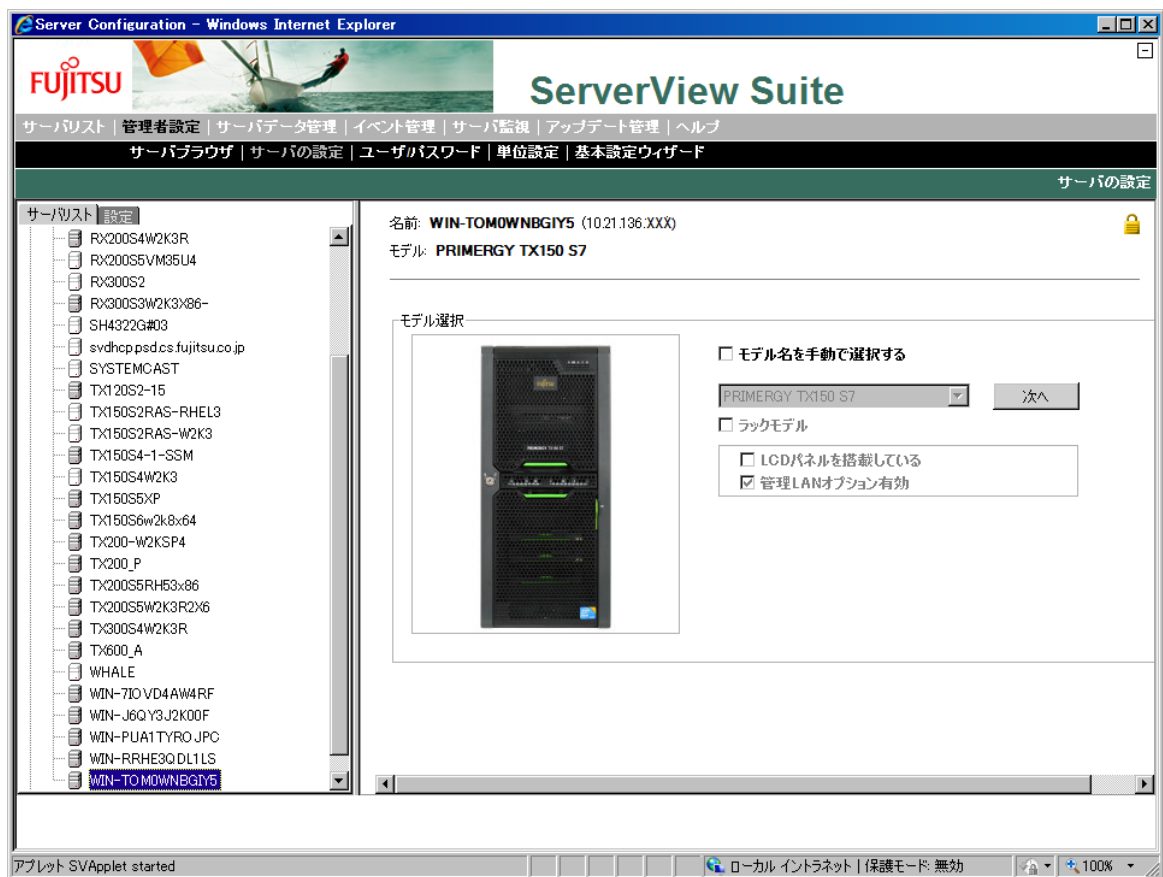



図 222：Operation Manager： サーバコンフィグレーションウィンドウ - 「サーバリスト」（2）タブ

➢ ウィンドウの右側に選択したサーバの詳細を指定し、［*次へ*］をクリックしてエントリを確定します。

「*Boot ウォッチドッグ*」ページを表す下記のウィンドウが表示されます（図 223 を参照してください）。

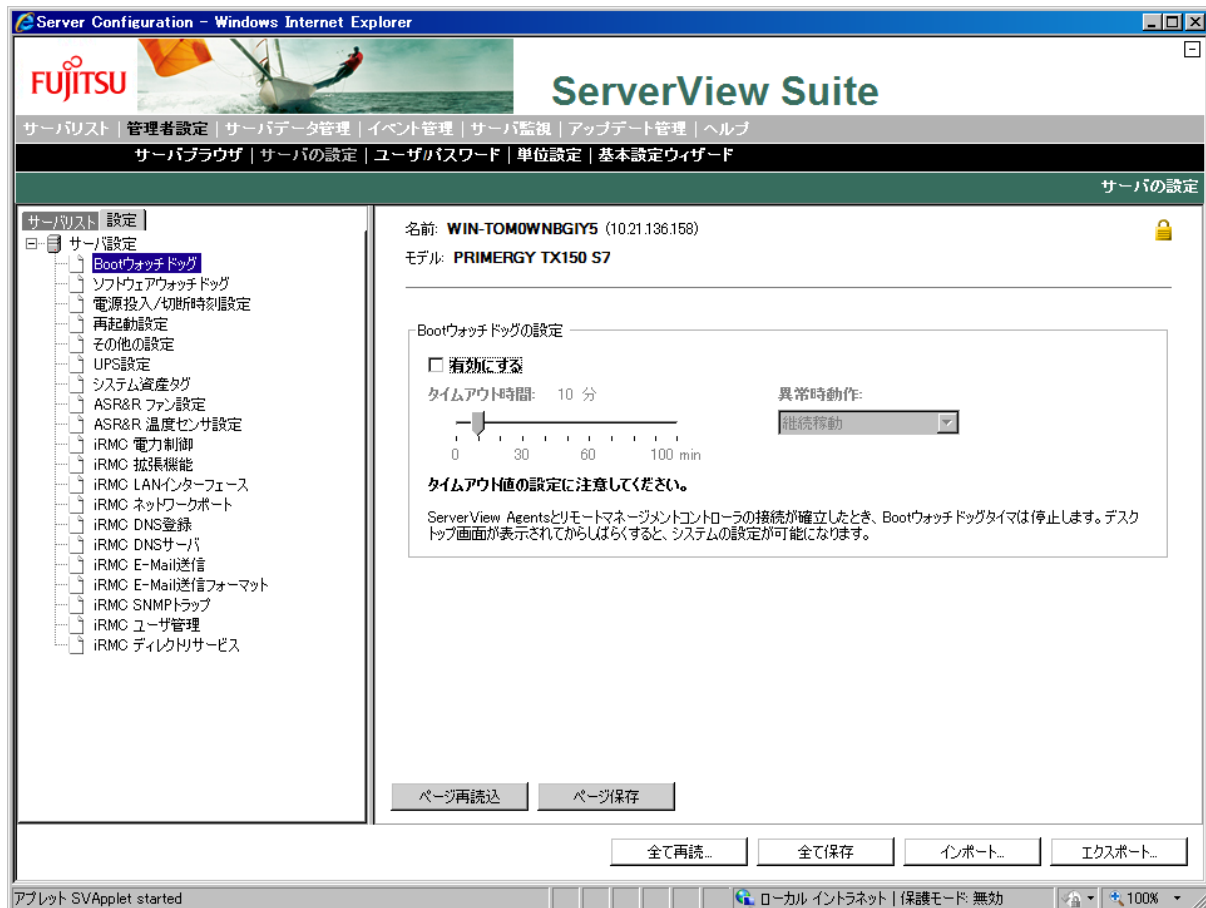



図 **223：Operation Manager**： サーバコンフィグレーションウィンドウ - 「管理者設定」タブ

➢ ナビゲーションエリアで、必要なファンクションをクリックします。すると関連ダイアログページがウィンドウの右側に表示されます。

本書では、**iRMC S2** の設定と、iRMC S2 にユーザー管理に関連があるダイアログページのみを説明します。

➢ 必要な設定を行い、［ページ保存］または［全て保存］でセーブしてください。

設定した各々のサーバの設定を、［ページ保存］でダイアログページ毎にを別々に有効化するか、すべての設定を完了させたのち［全て保存］で有効化します。

設定を元の値にリセットするには[ページ再読込]または[全て再読]を選択し ます。

サーバの設定が完了したら、「サーバリスト」タブから別のサーバを選択して設定作業を続けることができます。

9.2 iRMC Power Consumption Control - サーバ電力制御設定

「*iRMC* 電力制御」ダイアログページから、iRMC S2 が PRIMERGY サーバの消費電力を制御するのに使用するモードを指定することができます。

➢「*iRMC* 電力制御」を選択します。

名前: **WIN-TOM0WNBGIY5** (10.21.136.XXX)
モデル: **PRIMERGY TX150 S7**

電力制御オプション

電力制御: スケジュール
消費電力監視単位: Watt
消費電力モニタリング有効: ☑

Power Consumption Scheduler

Schedule 1:			Schedule 2:		
☐ 日曜	09:00	性能優先動作	☑ 日曜	08:30	省電力動作
☐ 月曜	00:00	電力制御無効	☐ 月曜	00:00	電力制御無効
☐ 火曜	00:00	電力制御無効	☐ 火曜	00:00	電力制御無効
☐ 水曜	00:00	電力制御無効	☐ 水曜	00:00	電力制御無効
☐ 木曜	00:00	電力制御無効	☐ 木曜	00:00	電力制御無効
☐ 金曜	00:00	電力制御無効	☐ 金曜	00:00	電力制御無効
☐ 土曜	00:00	電力制御無効	☐ 土曜	00:00	電力制御無効

ページ再読込 ページ保存

図 224 :「iRMC 電力制御」ダイアログページ

➢ 以下の設定をおこなってください。

「*消費電力モニタリング有効*」

電源監視を実施するかどうかを指定します。

i この設定は電源監視をサポートする PRIMERGY サーバのみで有効になります。

i 「消費電力モニタリング有効」はバージョン 3.32 のファームウェアでは初期値として有効に設定されます。

「*電力制御オプション*」
管理対象サーバの電力制御を管理するモードです。

– 「*電力制御無効*」
iRMC S2 は電力制御管理をオペレーティングシステムに委ねます。

– 「性能優先動作」
iRMC S2 はサーバが最高性能を発揮できるように設定します。この場合は、消費電力は大きくなる場合があります。

– 「省電力動作」
iRMC S2 はサーバの消費電力が可能な限り小さくなるように設定します。この場合は、サーバ性能は最大にはなりません。

– 「スケジュール」
iRMC S2 は電力制御を、電力制御スケジューラを基にして（下記参照）設定します。

「*スケジュール*」

i 「スケジュール」は、「電力制御オプション」で「スケジュール」オプションを選択した場合のみ有効です。

「スケジュール」を適用すれば、管理対象サーバの電力制御を iRMC S2 が管理する詳細なスケジュールとモード（オペレーティングシステムによる管理、最高性能、最少消費電力）を指定することができます。

9.3 iRMC の拡張機能 - リモートストレージサーバ、ライセンスキー、および、HP Systems Insight Manager との連携

iRMC の「*iRMC* 拡張機能」ダイアログページを使用すれば以下のタスクを実行できます。

– リモートストレージサーバの IP アドレスまたは DNS 名を iRMC S2 上に保存します。
– ビデオリダイレクションとリモートストレージ機能使用のためのライセンスキーを入力します。
– HP Systems Insight Manager との連携を有効または無効とします。

➢「*iRMC* 拡張機能」を選択してください。

名前: WIN-TOM0WNBGIY5 (10.21.136.XXX)
モデル: PRIMERGY TX150 S7

リモートイメージサーバ
ホスト名もしくはIPアドレス:

ライセンスキー
追加機能を有効にする場合には、ライセンスキーを入力してください。
キーは XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XX のような形式です。
ライセンスキー:

HP System Insight Manager (HP SIM)連携オプション
SIM連携を無効にする (再起動要)

ページ再読込　ページ保存

図 225 :「iRMC 拡張機能」ダイアログページ

➢ 以下の設定をおこなってください。

「ホスト名もしくは *IP* アドレス」
ここで、リモートストレージサーバがインストールされたコンピュータの DNS 名または IP アドレスを入力します。

「*ライセンスキー*」
ここでビデオリダイレクションとリモートストレージ機能使用のための有効なライセンスキーを入力します。

「*SIM 連携を無効にする ...*」
このオプションの有効／無効を切り換えて、HP SIM 連携を有効または無効にします。

「*SIM* 連携を無効にする ...」オプションを無効に設定すると、iRMC S2 は未認証 XML クエリに対する HP Insight Manager からの ID 情報に応答します。

9.4 ASR&R 冷却ファン設定

「*ASR&R* ファン設定」ダイアログページには、管理対象サーバの冷却ファンに関する情報が表示されます。個々の冷却ファンごとに、ファンの故障が発生した場合にサーバをシャットダウンするかどうか指定することができます。

➢ 「*ASR&R* ファン設定」を選択してください。

図 226 :「*ASR&R ファン設定」ダイアログページ*

➢ 以下の設定をおこなってください。

「異常時動作」

対応する冷却ファンが故障した場合にサーバをシャットダウンするかどうか指定し ます。

「*続行*」

サーバをシャットダウンしません。

「*シャットダウン＆電源断*」

「*シャットダウン待ち時間 (秒)* 」に指定された時間が経過しても冷却ファンの故障が続いていればサーバをシャットダウンします。

「*シャットダウン待ち時間 (秒)*」

「異常時動作」で「シャットダウン＆電源断」を選択した場合は、待ち時間をここに指定します。

サーバは関連する冷却ファンが故障し、指定された時間が経過しても故障が続いている場合にはシャットダウンされます。

この数値を入力しなければ、サーバは冷却ファンの故障直後にシャットダウンされます。

「*全ファンの異常時動作設定*」

ここで、すべての冷却ファンを対象として、いずれかのファンの故障が発生した場合にサ ーバをシャットダウンするかどうか指定することができます。

「続行」

サーバをシャットダウンします。

「シャットダウン＆電源断」

「シャットダウン待ち時間 (秒)」に指定された時間が経過しても故障した冷却ファンの以上が続いていればサーバをシャットダウンします。

9.5 ASR&R 温度センサ設定

「*ASR&R 温度センサ設定*」ダイアログページには、管理対象サーバの温度センサに関する情報が表示されます。致命的な温度のしきい値に達した場合にサーバをシャットダウンするかどうかを、センサ毎に指定することができます。

➤「ASR&R 温度センサ設定」を選択してください。

図 227 :「ASR&R 温度センサ設定」ダイアログページ

➤ 以下の設定をおこなってください。

「異常時動作」

選択したセンサが致命的な温度のしきい値に達した場合にサーバをシャットダウンする かどうかを指定します。

「続行」

サーバをシャットダウンしません。

「シャットダウン＆電源断」

サーバをシャットダウンします。

「全ファンの異常時動作設定」

すべてのセンサを対象として、いずれかのセンサが致命的な温度のしきい値に達した場合にサーバをシャットダウンするかどうかをここに指定することができます。

「続行」

サーバをシャットダウンしません。

「シャットダウン＆電源断」

サーバをシャットダウンします。

9.6 iRMC LAN インターフェース - Irma S2 の LAN パラメータの設定

iRMC S2 LAN パラメータの設定（イーサネットの設定）には「*iRMC LAN Interface*」ダイアログページを使用します。

注意！

LAN 設定を変更する前にシステムのネットワーク管理責任者に連絡してください。

iRMC S2 に不正な LAN パラメータを設定すると、以降での iRMC S2 へのアクセスには特殊な設定ソフトウェアを使用するか、シリアルインターフェースまたは BIOS 経由でアクセスせざるを得なくなります。

➢「iRMC LAN インターフェース」を選択してください。

名前: **WIN-TOM0WNBGIY5** (10.21.136.XXX)
モデル: **PRIMERGY TX150 S7**

☑ IPアドレスの設定を自動で取得する(DHCP)
以下のIPアドレスを使う
IPアドレス:
サブネットマスク:
デフォルトゲートウェイ:

LANインターフェース
LANポート: 共用LANポート
LAN接続速度: 自動検出

☐ VLAN有効
VLAN構成
VLAN ID: 0
VLANプライオリティ: 0

ページ再読込　ページ保存

図 228：「iRMC LAN インターフェース」ダイアログページ

➢ 以下の設定をおこなってください。

「P アドレスの設定を自動で取得する (DHCP)」

*「IP アドレスの設定を自動で取得する (DHCP)」*を有効にすると、iRMC S2 は LAN 設定をネットワーク上の DHCP サーバから自律的に取得します。この場合は、*IP* アドレス、サブネットマスク、および、デフォルトゲートウェイの値は自動的に設定されます。

DHCP サーバを使用できない場合は DHCP のオプションを有効にしてはなりません。DHCP サーバがないにもかかわらず DHCP のオプションを有効にした場合は、iRMC S2 はサーチループに入り込みます（すなわち、DHCP サーバを探し続けます。）

DHCP と DNS サービスの使用は、最初に以下のダイアログページのインストールが終わってから指定します。
iRMC DHCP DNS 設定（411 ページ参照）および
iRMC DNS サーバ設定（413 ページ参照）または
iRMC S2 Web インターフェースによりこれらの設定を行います。（289 ペー ジ、「ネットワーク設定 – LAN パラメータの設定」の節を参照してください。）初期設定では、iRMC S2 を最初にインストールするときに以下の名前が DHCP サーバに渡されます。iRMC<MAC アドレスの末尾の 3 バイト >。

「IP アドレス」

iRMC S2 の LAN 上のアドレスです。このアドレスは、管理対象サーバの IP アドレスとは別のものです。

このエントリは、DHCP が無効である場合のみ確認されます。（上記、「*IP* アドレスの設定を自動で取得する *(DHCP)*」を参照してください。）

「サブネットマスク」

このエントリは、DHCP が無効である場合のみ確認されます。（上記、「*IP* アドレスの設定を自動で取得する *(DHCP)*」を参照してください。）

iRMC S2 の LAN 上のサブネットマスクです。

「デフォルトゲートウェイ」

iRMC S2 の LAN 上のデフォルトゲートウェイです。

このエントリは、DHCP が無効である場合のみ確認されます。（上記、「*IP* アドレスの設定を自動で取得する *(DHCP)*」を参照してください。）

「LAN 接続速度」

LAN 接続速度。以下のオプションを使用可能です :

– 自動検出
– 100 MBit/ 秒 全二重
– 100 MBit/ 秒 半二重
– 10 MBit/ 秒 全二重
– 10 MBit/ 秒 半二重

*「自動検出」*を選択すると、iRMC S2 に割り当てられたオンボード LAN コントローラが、接続されるネットワークポートの適切な速度と二重化方式を自動的に判定します。

「LAN ポート」

このオプションは、PRIMERGY サーバではサポートされていません。

一部の PRIMERGY サーバモデルでは搭載されたシステム NIC （ネットワークインターフ ェースカード）の LAN インターフェース を以下のように設定することができます。

– システムと共用運用するためのシェアード LAN として

または

– 管理用 LAN 専用のサービス LAN として

PRIMERGY サーバ、タイプ TX150 S6 ではサービス LAN が必須です。

「VLAN 有効」

このオプションによって、iRMC S2 の VLAN サポートが有効となります。

「VLAN ID」

iRMC S2 が所属するバーチャルネットワーク（VLAN）の VLAN ID 数値許容範囲： 1□ VLAN Id □ 4094

「VLAN プライオリティ」

VLAN ID により指定された VLAN 中の iRMC S2 の VLAN 優先度(ユーザー優先度）数値許容範囲: 0 VLAN 優先度 7（初期値： 0)

9.7 iRMC ネットワーク用ポート - ポート番号とネットワークサービスの設定

「*iRMC ネットワークポート*」ダイアログページによって、ポート番号とネットワークサービス設定の設定を表示させ変更することができます。

注意！
iRMC S2 Web インターフェースにより入力領域が無効にされたポート番号の設定はサポートされません。（293 ページを参照してください。）iRMC S2 Web インターフェースを使用してポート番号を設定することが可能であるかどうかの判定のみが可能となります。最初に設定する間に Server Configuration Manager を使用して現在の値から変更してはなりません。

➢ iRMC ネットワーク用ポート番号の選択。

図 229 :「iRMC ネットワークポート」ダイアログページ

➢ 以下の設定をおこなってください :

「*HTTP ポート*」
　　iRMC S2 の HTTP ポート（セキュリティ保護されない接続）

「*HTTPS* ポート」
　　iRMC S2 の HTTPS ポート（セキュリティ保護される接続）

「HTTPS 接続のみ有効」

「*HTTPS* 接続のみ有効」オプションを無効にすると、ユーザーは、iRMC S2 に入力領域に指定した HTTP ポートとのセキュリティ保護されない接続の確立しかできなくなります。

「*HTTPS* 接続のみ有効」オプションを有効にすると、ユーザーは、iRMC S2 に入力領域に指定した HTTPS ポートとのセキュリティ保護される接続の確立が可能となります。

iRMC S2 Web インターフェースでウェブのアクセスの設定もできます。SSL 証明書の期限が切れている場合は、ウェブブラウザにこの問題に関するメッセージが表示されます。

「Telnet 有効」

強制「Telnet 有効」オプションを有効にすると、ユーザーは、iRMC S2 に入力領域に指定した Telnet ポートとの接続の確立が可能となります。

「Telnet ポート」

iRMC S2 の Telnet ポートこの入力領域は、「Telnet 有効」が有効になっている場合のみ表示されます。

「SSH ポート」

iRMC S2 の SSH ポート

「Telnet ドロップアウト時間 (秒)」

Telnet 接続が自動的に切断された後の使用不可能になる時間（秒）。

「標準ポート」

iRMC S2 の VNC ポート、固定設定（ポート番号： 80）

「セキュアポート」

iRMC S2 の セキュリティ保護された VNC ポート、固定設定（ポート番号： 443).

「リモートストレージポート」

iRMC S2 のリモートストレージポート

9.8 iRMC DNS 登録 - iRMC S2 のホスト名のサーバの設定を使った設定

「*iRMC DNS* 登録」ダイアログページを使用して、iRMC S2 にホスト名を設定し、「ダイナミック *DNS*」が使用できるようにします。「dynamic DNS」を使用すれば、IP アドレスと DNS サーバが識別し易くなるようにネットワークコンポーネントのシステム名が DHCP サーバから自律的に発行されます。

➢ 「iRMC DNS 登録」を選択します。

図 230： 「iRMC DNS 登録」ダイアログページ

➢ 以下の設定をおこなってください。

「DHCP アドレスを DNS に登録」
　　iRMC S2 用 DHCP サーバへの DHCP 名の転送を有効／無効にします。

「シリアル番号を付加する」
　　iRMC S2 の MAC アドレスの末尾 3 バイトが、iRMC S2 の DHCP 名の末尾に追加されます。

「ホスト名に iRMC を使用する」
　　「iRMC 名」入力領域に指定された iRMC 名をサーバ名の代わりに、iRMC S2 に使用します。

「iRMC 名」

サーバ名に変わって DHCP に渡される iRMC S2 の iRMC 名。

「文字列を付加する」

「文字列」入力領域に指定された拡張子は、iRMC S2 の DHCP 名に追加されます。

「文字列」

iRMC S2 の名前の拡張子を入力します。

9.9 iRMC DNS サーバ - iRMC S2 の DNS の有効化

「iRMC DNS サーバ」ダイアログページによって、iRMC S2 のドメイン名サービス（DNS）を有効にすることができます。その結果、iRMC S2 の設定に IP アドレスに代わって DNS シンボリック名 を使用することができます。

➤ 「iRMC DNS サーバ」を選択します。

図 231 :「iRMC DNS サーバ」ダイアログページ

➤ 以下の設定をおこなってください。

「DNS 有効」
　　iRMC S2 の DNS を有効／無効にします。

「DHCP から DNS 構成を取得する」
　　このオプションを有効にすると、DNS サーバの IP アドレスは DHCP サーバから自動的に取得されます。この場合には、最大 5 台の DNS サーバがサポートされます。 この設定を有効にしない場合には、「DNS サーバ 1 – DNS サーバ 5」の下で最大 5 台の DNS サーバのアドレスをマニュアルで入力できます。

「*DNS* ドメイン」

*「DHCP から DNS 構成を取得する」*オプションを無効にした場合は、DNS サーバにリクエストするためのデフォルトドメインの名前を指定します。

「*DNS* サーバ *1 ..5*」

*「DHCP から DNS 構成を取得する」*オプションを無効にした場合は、最大 5 台の DNS サーバの名前をここに入力できます。

9.10 iRMC Email 送信 - Email 警告の設定

*「iRMC Email 送信」*ダイアログページを使用して、iRMC S2 が Email を送信する方法を設定します。

➢ 「iRMC Email 送信」を選んでください。

図 232 :「iRMC Email 送信」ダイアログページ

➢ 以下の設定をおこなってください。

「E-mail での警告送信を有効にする」
　　このオプションを有効にします。

「SMTP 設定」
　ここでグローバル Email 設定をおこないます。

「SMTP リトライ回数」
　　SNMP リトライ回数

「SMTP リトライ間隔 (秒)」
　　SNMP リトライの間隔時間

「*SNMP 応答待ち時間 (秒)*」

SMTP レスポンスのタイムアウト（秒単位）

「*プライマリ SMTP サーバ設定*」

ここでプライマリ SMTP サーバ（SMTP サーバ）設定をおこないます。

「*SMTP サーバ*」
プライマリメールサーバの IP アドレス

iRMC S2 用のドメインネームサービス （DNS）を有効化することができます。
（413 ページ、「iRMC DNS サーバ - iRMC S2 の DNS の有効化」を参照してください。）
IP アドレス の代わりにシンボリックネームを使用することができます。

「*SMTP ポート*」
プライマリメールサーバの SMTP ポート

「*認証タイプ*」
iRMC S2 をプライマリメールサーバに接続する際の認証タイプ。
– 「認証を行わない」
接続に認証を使用しない
– 「認証を行う (RFC 2554)」
RFC 2554 に準拠する認証、認証のための SMTP サービスの拡張

「*認証ユーザー名*」
プライマリメールサーバ上の認証用ユーザー名

「*パスワード*」
プライマリメールサーバ上の認証用パスワードを入力します。

「*パスワード確認*」
ここでもう一度パスワードを入力します。

「*セカンダリ SMTP サーバ設定*」
ここでセカンダリ SMTP サーバ（SMTP サーバ）設定を構成します。

「*SMTP* サーバ」
セカンダリメールサーバの IP アドレス

iRMC S2 用のドメインネームサービス （DNS）を有効化することができます。
（413 ページ､「iRMC DNS サーバ - iRMC S2 の DNS の有効化」の節を参照してください。）
IP アドレスの代わりにシンボリックネームを使用することができます。

「*SMTP ポート*」
セカンダリメールサーバの SMTP ポート

「*認証タイプ*」
iRMC S2 をセカンダリメールサーバに接続する際の認証タイプ。

- 「認証を行わない」
  接続に認証を使用しない
- 「認証を行う (RFC 2554)」
  RFC 2554 に準拠する認証、認証のための SMTP サービスの拡張

「*認証ユーザー名*」
セカンダリメールサーバ上の認証用ユーザー名

「*パスワード*」
セカンダリメールサーバ上の認証用パスワードを入力します。

「*パスワード確認*」
確認のためにもう一度パスワードを入力します。

9.11 iRMC E-Mail 送信フォーマット - E-mail 送信フォーマットの設定

「*iRMC E-mail* 送信フォーマット」ダイアログページを使用して *E-mail* 送信フォーマットの設定をおこないます。「*iRMC* ユーザー管理」ダイアログページの「ユーザーの修正」ウィンドウを使用して各ユーザーのメールフォーマットを指定します。(422 ページを参照してください)

以下の E-mail フォーマットがサポートされます。

– 標準メール

– 題名固定

– ITS- フォーマット

– 富士通 REMCS フォーマット

➤「iRMC E-mail 送信フォーマット」を選んでください。

名前: **WIN-TOM0WNBGIY5** (10.21.136.XXX)

モデル: **PRIMERGY TX150 S7**

E-Mail送信フォーマット

送信元: MailFrom@domain.com

題名: test

本文:

管理者名:

管理者電話番号:

送信元サーバURL:

ページ再読込　ページ保存

図 233 :「iRMC E-mail 送信フォーマット」ダイアログページ

➢ 以下の設定をおこなってください。（メールのフォーマットによっては一部の入力領域は無効となります。）

「送信元」

iRMC S2 送信者 ID
すべてのメールフォーマットに有効です。

ここに入力された文字列に「@」が含まれていれば文字列は有効な Email アドレスと解釈されます。「@」がない場合には有効な Email アドレスとして「admin@<ipaddress>」が使用されます。

「*題名*」

警告メールの題名。
メールフォーマットが固定題名の場合のみ有効となります。(425 ページを参照してください。)

「*本文*」

メッセージのタイプ（Email)。
メールフォーマットが固定題名の場合のみ有効となります。(425 ページを参照してください。)

「*管理者名*」

管理者の名前（任意）
メールフォーマットが ITS メールフォーマットの場合のみ有効となります。（425 ページを参照してください。）

「*管理者の電話番号*」

管理者の電話番号（任意）
メールフォーマットが ITS メールフォーマットの場合のみ有効となります。（425 ページを参照してください。）

「*REMCS ID*」

この ID は追加のサーバ ID です。シリアル番号と同様です。
メールフォーマットが「*Fujitsu REMCS* フォーマット」の場合のみ有効となります。（425 ページ を参照してください。）

「*送信元サーバ URL*」

特定の条件下でサーバがアクセスできる URL です。
URL はマニュアルで入力する必要があります。
標準メールフォーマットの場合のみ有効となります。(425 ページを参照してください。)

9.12 iRMC SNMP トラップ - 設定 SNMP トラップ警告

「*iRMC SNMP* トラップ」ダイアログページから、SNMP トラップ警告の設定を表示させて設定することができます。

最大 7 台までの SNMP サーバ宛の SNMP トラップ発信がサポートされます。

➢「iRMC SNMP トラップ」を選んでください。

名前: **WIN-TOM0WNBGIY5** (10.21.136.XXX)

モデル: **PRIMERGY TX150 S7**

SNMPコミュニティ:

SNMPトラップ送信先 (ホスト名もしくはIPアドレス)

SNMPサーバ 1:

SNMPサーバ 2:

SNMPサーバ 3:

SNMPサーバ 4:

SNMPサーバ 5:

SNMPサーバ 6:

SNMPサーバ 7:

ページ再読込　ページ保存

図 234： 「iRMC SNMP トラップ」ダイアログページ

➢ 以下の設定をおこなってください。

「*SNMP* コミュニティ」
: SNMP コミュニティの名前

「*SNMP* トラップ送信先（ホスト名もしくは *IP* アドレス)」
: このコミュニティに属し「トラップ送信先」として設定されるサーバの DNS 名または IP アドレス

9.13 iRMC ユーザー管理 - iRMC S2 上のローカルユーザー管理

「*iRMC* ユーザー管理」ダイアログページを使用して、iRMC S2 のローカルユーザー管理を設定することができます。

このダイアログページには設定されたユーザーがリスト表示されます。各行に設定されたユーザーが一つずつ入ります。

iRMC S2 上のユーザー管理には「ユーザーアカウント変更権限」が必要です。

ユーザー ID 1（「null user」）は IPMI 規格にリザーブされますので、iRMC S2 上のユーザー管理には使用できません。

➢iRMC ユーザー管理を選択します。

図 235 :「iRMC ユーザー管理」ダイアログページ

➢ ユーザーを削除するには、先ずユーザーを選択し（対応する行を選択)、以下に［削除 ...］ボタンをクリックして、ユーザーの削除を確認します。

➢ ユーザー ID がまだどのユーザーにも割り当てられていない行（空白行）をダブルクリック、または、その行を選択して［修正 ...］ボタンを押下し、空白の「ユーザーの修正」ウィンドウ（初期値に設定されています）を開いて、新しいユーザーの設定を行います。（図 236 を参照してください。）

➢ 特定ユーザーの行をダブルクリックするか、ユーザーを選択して［修正 ...］ボタンを押下し、「ユーザーの修正」ウィンドウを開いてそのユーザーの設定を表示させ、変更をすることができます。（図 236 を参照してください。）

ユーザの修正

☑ アカウントを有効にする

アカウント有効期限

ユーザ名: admin

ユーザの説明: User 02 Description

パスワード: *****

パスワード確認: *****

ユーザ権限

LAN: OEM

シリアル: OEM

☑ ユーザの設定をすることができます　☑ ビデオリダイレクションを使うことができます

☑ iRMCの設定をすることができます　☑ リモートストレージを使うことができます

ユーザシェル

シェル: リモートマネージャ

EMailページング設定

フォーマット: 通常　☑ 有効

アドレス: User02@domain.com

優先サーバ: 自動

ファンセンサ: 警告　温度センサ: 警告

ハードウェアエラー: 全て　システムハング: 注意

POSTエラー: 全て　セキュリティ: 警告

システムステータス: なし　ディスクコントローラ: 注意

ネットワークエラー: 警告　リモートマネジメント: 注意

システム電源: 警告　メモリ: 注意

その他のエラー: なし

OK　キャンセル

図 236 :「ユーザーの修正」ウィンドウ

「*アカウントを有効にする*」
　　このオプションを無効にするとユーザーはロックされます。

「*アカウントデータ*」
　　ユーザーのアクセスデータをここで設定します。

「*ユーザー名*」
　　ユーザーの名前を入力します。

「*ユーザーの説明*」
　　ユーザーの付加的な情報

「*パスワード*」
　　ユーザーのパスワードを入力します。

「*パスワード確認*」
　　確認のためにもう一度パスワードを入力します。

「*ユーザー権限*」
　　ここでチャンネル固有のユーザー権限を他の権限と合わせて設定します。

「*LAN*」
　　ユーザーに対する LAN チャンネルの権限グループを割り当てます。
　　以下のオプションを使用可能です。
　　– User
　　– Operator
　　– Administrator
　　– Administrator – OEM
　　権限グループに関連する権限に関する情報は、56 ページ、「ユーザー権限」の節を参照してください。

「*シリアル*」
　　ユーザーに対する シリアルチャンネルの権限グループを割り当てます。LAN 権限と同じ権限グループを使用することができます。

「*ユーザーの設定をすることができます*」
　　ユーザークセスデータを設定する権限

「*iRMC の設定をすることができます*」
　　iRMC S2 設定の設定する権限

「*ビデオリダイレクションを使うことができます*」
　　ビデオリダイレクション（AVR）を「ビューモード」または「フルコントロールモード」で使用する権限。

「*リモートストレージを使うことができます*」
Remote Storage 機能を使用する権限

「*ユーザーシェル*」
ここでユーザーシェルを選択します。

「*シェル*」
ここで使用したいユーザーシェルを選択します。

以下のオプションを使用可能です：

– SMASH CLP
381 ページ、「コマンドラインシェルの起動 ... - SMASH CLP シェルの起動」の節を参照してください。

– リモートマネージャ
361 ページ、「Telnet/SSH アクセス（Telnet/SSL での管理）」の章を参照してください。

– IPMI ベーシックモード

– IPMI ターミナルモード

– なし

「*E-mail ページング設定*」
Email フォーマットを規定する設定とグローバル Email の設定をここで構成します。

「*有効*」
ユーザーに Email でシステムの状態を通知するかどうか指定します。

「*フォーマット*」

選択した Email のフォーマットにしたがって、「iRMC E-mail 送信フォーマット」ダイアログページでさまざまな設定を行うことができます。(417 ページを参照してください。)

以下の Email フォーマットが使用可能です :

– 通常

– 決定済 Subject

– ITS フォーマット

– Fujitsu REMCS フォーマット

iRMC S2 のイベントログのすべてのエントリは特定のページンググループに割り当てられます。

「*アドレス*」

受信者の Email アドレス

「*優先サーバ*」

優先メールサーバを選択します。
以下のオプションからひとつを選択します :

– *自動*

Email が即時適切に送られない場合、たとえば優先メールサーバが使用不可能な場合には、Email は 2 番目のメールサーバに送られます。

– *プライマリ*

プライマリ SMTP サーバとして設定した SMTP サーバ（416 ページ参照）のみが優先メールサーバとして使用されます。

– *セカンダリ*

セカンダリ SMTP サーバとして設定した SMTP サーバ（417 ページ参照）のみが優先メールサーバとして使用されます。

Email 送信時のエラーはイベントログに記録されます。

「ユーザーの修正」ウィンドウの下 3 分の 1 の部分では、iRMC S2 ユーザーに Email で通知されるシステムイベントを設定できます。(「E-mail ページング設定」)。

「なし」
: このページンググループには通知機能は無効とされます。

「*注意*」
: iRMC S2 は、システムイベントログのエントリに警告が報告されたときにユーザーに通知します。

> **i** 警告が設定されている場合は、状態が致命的と報告されたシステムイベントログのエントリもユーザーに通知します。

「*警告*」
: iRMC S2 は、システムイベントログのエントリに致命的と報告されたときにユーザーに通知します。

「*すべて*」
: iRMC S2 はシステムイベントログにエントリが上げられる原因となるイベントすべ てをユーザーに通知します。

➢ 設定が終わったら［*OK*］をクリックして確定します。

9.14 iRMC ディレクトリサービス - ディレクトリサービスの設定

「*iRMC* ディレクトリサービス」ダイアログページを使用すると、ディレクトリサービス経由で、iRMC S2 のグローバルユーザー管理を設定することができます。(77 ページを参照してください。)

現在は､以下のディレクトリサービスをサポートする iRMC S2 LDAP アクセスがサポートされています。Microsoft Active Directory、および OpenLDAP

以下の記号は、LDAP 上で文字列を検索するためのメタキャラクタとして指定されています &, |, !, =, <, >, ~, :

したがって、ユーザーはこれらの記号を相対識別名（RDN）の要素として使用することはできません。

➢「iRMC ディレクトリサービス」を選択します。

図 237 「iRMC ディレクトリサービス」ダイアログページ

「*LDAP を有効にする*」

このオプションは、iRMC S2 が LDAP 経由でディレクトリサービスにアクセスできるかどうかを指定します。

LDAP 経由のディレクトリサービスアクセスは、「LDAP 有効」が有効になっている場合のみ可能です。「LDAP 有効」にチェックが付けられると、ログイン情報（210 ページ参照）はウェブブラウザと、iRMC S2 の間で SSL 暗号化されて必ず転送されます。

「*ローカル ID でのログインを無効化する*」

このオプションを有効にすると、ローカルのすべての iRMC S2 ユーザー ID はロック され、ディレクトリサービスにより ID を管理されるユーザーのみが有効になります。

注意！
「ローカル ID でのログインを無効化する」オプションが有効な場合は、ディレクトリサービスの接続は失敗しその後 iRMC S2 のログインできなく なります。

「*常に SSL ログインを使用する*」

このオプションは、LDAP が無効になっている場合のみ意味を持ちます。

このオプションを有効にすると、もし、LDAP が無効化されていたとしても、必ず HTTP SSL- セキュリティ保護ログインページを使用します。「常に SSL ログインを使用する」が有効とされず、LDAP が無効にされている場合は、「Digest Authentication Login」によりセキュリティ保護されたマスクが使用されます。

➢「LDAP 有効」オプションの有効化。

➢「ディレクトリサーバタイプ」から必要なディレクトリサービスを選んでください。

選択したディレクトリサービスによって、ことなる入力領域が規定されます。

– Active Directory の場合は、429 ページの「iRMC S2 の Microsoft Active Directory 用設定」の節を参照してください。

– OpenLDAP の場合は、431 ページの「iRMC S2 の Novell eDirectory / OpenLDAP 用設定」の節を参照してください。

9.14.1 iRMC S2 の Microsoft Active Directory 用設定

図 238 の例に記されたエントリに関しては、100 ページ、「Microsoft Active Directory に よる iRMC S2 ユーザー管理」の節を参照してください。

名前: WIN-TOM0WNBGIY5 (10.21.136.XXX)
モデル: PRIMERGY TX150 S7

☐ 常にSSLログインを使用する
☑ LDAPを有効にする　　☐ ローカルIDでのログインを無効にする

LDAP設定

ディレクトリサーバタイプ: Active Directory
LDAPサーバ 1: 0.0.0.0
LDAPサーバ 2: 0.0.0.0
ドメイン名: domain.com
部署名: department
☑ LDAP SSL 有効
ベースDN: ou=myorganization,ou=mycompany
ベースDN配下のグループディレクトリ:
ユーザ検索:

ディレクトリ サービス アクセス構成

LDAP認証 ユーザ名: LDAPuserName
LDAP認証 パスワード: *************
****
プリンシパルユーザDN: OU=
☐ ベースDNをプリンシパルユーザDNに追加する
☐ 拡張ユーザログイン
ユーザログイン検索フィルタ: (&(objectclass=person)(cn=%s))

LDAP通知設定

E-Mail通知有効: ☑
LDAP通知更新: 2 時間

ページ再読込　ページ保存

図 238：「iRMC ディレクトリサーバ（Microsoft Active Directory）」ダイアログページ

➢ 残りの設定をおこなってください。

「*LDAP サーバ 1*」

使用される LDAP ディレクトリサーバの IP アドレスと DNS 名

「*LDAP サーバ 2*」

バックアップサーバとして保守管理され *LDAP* サーバ *1* が故障した時にディレクトリサーバとして使用される LDAP ディレクトリサーバの IP アドレスと DNS 名

「*ドメイン名*」

ディレクトリサーバの完全な DNS パス名

「*部署名*」

部署名。ディレクトリサービスには、ユーザーのアクセス許可を判断するために部署名が必要です。ユーザーは、たとえば部署 X のサーバと部署 Y のサーバで異なるパーミッションを与えられる場合もあります。（あわせて 84 ページの図 27 も参照してください。）

「*LDAP SSL 有効*」

このオプションにチェックをつけると、iRMC S2 とディレクトリサーバの間のデータ転送は SSL 暗号化されます。

i 「*LDAP SSL* 有効」は、iRMC S2 Web インターフェースのページが開かれたときに SSL で保護されているかどうかには、影響を与えません。

i 「*LDAP SSL* 有効」はドメインコントローラ証明書がインストールされている場合のみ有効としてください。

「*ベース DN*」

「ベース DN」はドメイン名から自動的に派生します。

「*LDAP 認証 ユーザー名*」

これらの設定は現状では意味を持ちません。
グローバルユーザー ID に関連がある警告には、この部分の設定が必要となります。しかしながら、警告がサポートされるのは現時点ではローカルのユーザー ID のみです。

➢［ページ保存］ボタンをクリックしてディレクトリサービスの設定を完了させ、設定を有効にしてください。

9.14.2 iRMC S2 の Novell eDirectory / OpenLDAP 用設定

Novell eDirectory は未サポートです。

> **i** 「ディレクトリサービス構成」ダイアログページは、Novell eDirectory と OpenLDAP では同じストラクチャとなります。

> **i** 図 239 の例に記されたエントリに関しては、109 ページ、「Novell eDirectory によるグ ローバル iRMC S2 ユーザー管理」の節を参照してください。

図 239 : 「iRMC ディレクトリサービス」ダイアログページ

➢ 残りの設定をおこなってください。

「*LDAP サーバ 1*」
使用される LDAP ディレクトリサーバの IP アドレスと DNS 名

「*LDAP サーバ 2*」
バックアップサーバとして保守管理され LDAP サーバ 1 が故障した時にディレクトリサーバとして使用される LDAP ディレクトリサーバの IP アドレスと DNS 名。

「*部署名*」
部署名。ディレクトリサービスには、ユーザークセス許可を判断するために部署名 ¥ が必要です。ユーザーは、たとえば部署 X のサーバと部署 Y のサーバで異なるアクセス許可を与えられる場合もあります。(あわせて 90 ページの図 27 も参照してください。)

「*LDAP SSL 有効*」
このオプションにチェックをつけると、iRMC S2 とディレクトリサーバの間のデータ転送は SSL 暗号化されます。

i 「*LDAP SSL* 有効」は、iRMC S2 Web インターフェースのページが開かれたときに SSL で保護されているかどうかには、影響を与えません。

i 「*LDAP SSL* 有効」はドメインコントローラ証明書がインストールされている場合のみ有効としてください。

「*ベース DN*」
「ベース DN」は eDirectory または OpenLDAP サーバの完全な識別名で、OU(組織単位) iRMCgroups を含むツリーまたはサブツリーを表します。この DN は、LDAP 検索の開始点となります。

「*ベース DN 配下のグループディレクトリ*」
OU iRMCgroups のパス名で、「ベース DN」のサブツリーです。

「*ユーザー検索*」
OU Users のパス名で、「ベース DN」のサブツリーです。

「*LDAP 認証*」、「*ユーザー名*」
一般的な iRMC S2 ユーザー ID。が iRMC S2 はその ID の下の iRMC S2 ユーザーの LDAP サーバの権限をクエリします。

「*LDAP 認証*」、「*パスワード*」
プリンシパルユーザーが、LDAP サーバから認証を取得しパスワードを確認するために使用するパスワード

「*プリンシパルユーザー DN*」

一般的な iRMC S2 ユーザー ID（プリンシパルユーザー）の完全な識別名。iRMC S2 はその ID の下の iRMC S2 ユーザーの LDAP サーバの権限をクエリします。

「*ベース DN をプリンシパルユーザー DN に追加する*」

このオプションを有効にすると、「プリンシパルユーザー *DN*」の下で「ベース *DN*」を指定する必要がありません。「ベース *DN*」により指定された基本 DN が適用されま す。

「*Bind DN*」

「*Bind DN*」は、LDAP 認証に使用されたプリンシパルユーザー DN を示します。

「*拡張ユーザーログイン*」

ユーザーログインのフレキシビリティを拡張します。
「拡張ユーザーログイン」を選択すると、「ユーザーログイン検索フィルタ」入力領域もあわせて有効になります。初期設定では、ここに標準ログイン検索フィルタが 含まれます。

ログイン時には、プレースホルダ「%s」は関連するグローバルログインに置き換えられます。

「*cn=*」に代わって別の属性を指定すれば、フィルタを変更することができます。すべてのグローバルログインは、この検索フィルタの基準に合致すれば、iRMC S2 にログインする権限が与えられます。

注意！
このオプションは、LDAP の構文に習熟している場合のみ有効にしてください。指定を誤り、使用できない検索フィルタを有効にしてしまうと、ユーザーは「拡張ユーザーログイン」オプションを無効にした後、ユーザーはグローバルログインの iRMC S2 にログインすることしかできなくなります。

➢ ［ページ保存］ボタンをクリックしてディレクトリサービスの設定を完了させ、設定を有効にしてください。

10 章 ファームウェアのアップデート

本章では、次の事項について説明しています。

– iRMC S2 ファームウェア（概要）

– ファームウェアアップデート用メモリスティックの作成

– ファームウェアイメージのアップデート

– エマージェンシーフラッシュ

– フラッシュツール

最新版のファームウェアは「ServerView Suite DVD 1」にあります。また、「Fujitsu Technology Solutions web server（富士通テクノロジーソリューション Web サーバ）」のダウンロードセクションから手動でダウンロードすることもできます。

最新版の「ServerView Suite DVD 1」は 2ヶ月ごとにお届けします。

ファームウェアをアップデートする前に、最新版のファームウェアの注意書き（特に Readme ファイル）をしっかりとお読みください。

アップデートしたファームウェアを起動するには、管理対象サーバを再起動する必要があります。

注意！
ファームウェアのアップデート時には、ランタイムファームウェアおよび SDR（Sensor Data Record）（→ P.437）が同一ファームウェアリリースのものである場合にのみファームウェアの正常な動作が保証されます。ご注意ください。

10.1 iRMC S2 ファームウェア（概要）

ファームウェアアップデート中もファームウェアが動作できるように、iRMC S2 は 2 種類の異なるファームウェアイメージを使用します。

2 種類のファームウェアは、16-MB EEPROM（**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory）に格納されています。

– ファームウェア 1
– ファームウェア 2

iRMC S2 のファームウェアは EEPROM ではなく、起動時に SRAM メモリにロードして実行されます。したがって、オンラインつまり Windows もしくは Linux といったサーバのオペレーティングシステムの実行中に、動作中のファームウェアと動作していないファームウェアの両方をアップデートすることができます。

iRMC S2 ファームウェアおよび EEPROM に関する情報は次の場所にあります。

– iRMC S2 Web インターフェースの「iRMC S2 情報」ページ（→ P.228）

– フラッシュツール（→ P.448）

アクティブおよびパッシブファームウェアイメージ

常時 2 種類のファームウェアイメージのうちのどちらかが動作しています。どちらのファームウェアイメージが実行されるかは、いわゆるファームウェアセレクタが決定します（→ P.438）。

iRMC S2 EEPROM の構造
iRMC S2 の EEPROM には、ファームウェアイメージ 1 用の領域とファームウェアイメージ 2 用の領域とがあります。

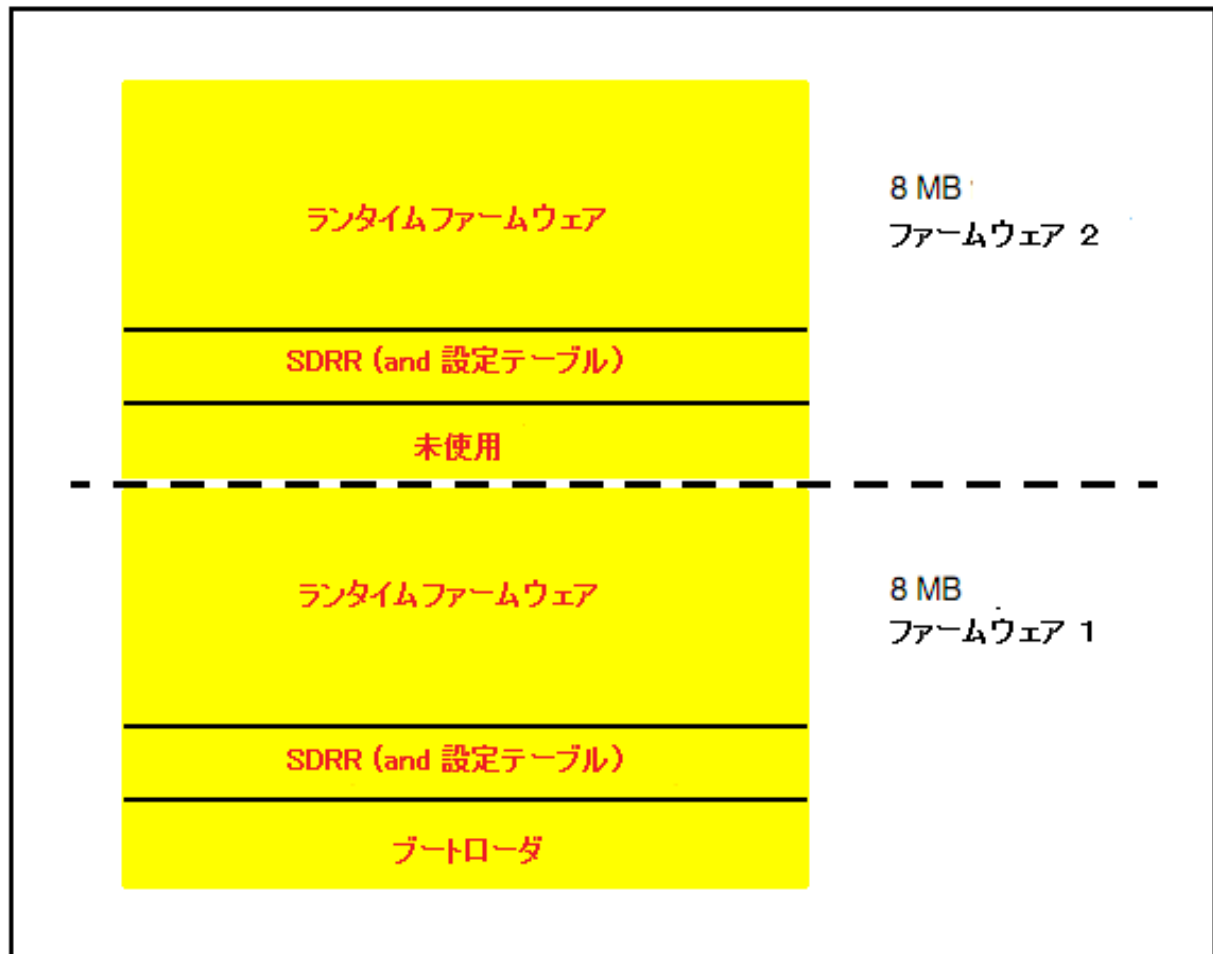



図 .240：iRMC S2 EEPROM の構造

– ブートローダ

ブートローダは、動作中のファームウェアイメージの状態確認を行います。ファームウェアエラー を発見すると、ファームウェアセレクタにもう一方のファームウェアイメージを設定します。

– SDRR（Sensor Data Record Repository）

SDRR 内の SDR（Sensor Data Records）には、管理対象サーバのセンサ情報が格納されています。また、SDRR は SDR にアクセスするためのインターフェースとしての役割も果たします。

– ランタイムファームウェア

iRMC S2 ファームウェアの実行可能部分です。.

この 3 つの領域に対して、ファームウェアのアップデートを行います。

ファームウェアセレクタ

ファームウェアセレクタが、実行する iRMC S2 を指定します。iRMC S2 が再設定および再起動されるたびに、対応するファームウェへのブランチを評価し処理します。

ファームウェアセレクタには、次の値があります。

0 自動－版数が新しいファームウェア

1 ファームウェア 1

2 ファームウェア 2

3 版数が古いファームウェア

4 書込日が新しいファームウェア

5 書込日が古いファームウェア

i 使用されたアップデートによって、アップデート後のファームウェアセレクタの設定は異なります。

ファームウェアセレクタを参照し明示的に設定するには、次の 2 つの方法があります。

– iRMC S2 Web インターフェースの「iRMC S2 情報」 ページ。「動作中のファームウェ ア」(→ P.230) を参照してください。

もしくは

– フラッシュツール（→ P.448）

10.2 USB メモリスティックの設定

i 次のいずれかの方法で、iRMC S2 のファームウェアをアップデートする場合には、USB メモリスティックは必要ありません。

– ServerView Update Manager
– ServerView Update Manager Express もしくは ASP
– iRMC S2 Web インターフェースおよび TFTP サーバ

次の手順にしたがって処理を行ってください。

➢「Fujitsu Technology Solutions web server（富士通テクノロジーソリューション Web サーバ）」のダウンロードセクションから、コンピュータのディレクトリ上に「iRMC Firmware Update for USB Stick」ファームウェアをダウンロードしてください。

もしくは

最新の「ServerView Suite DVD 1」をコンピュータの DVD ドライブに設定してください。

ダウンロードディレクトリもしくは DVD 1 上に、次のファイルもしくは ZIP アーカイブが見つかります。

– FTS_<*nnnnnnn*>.exe

– FTS_<*nnnnnnn*>.zip

ZIP アーカイブ内には、次のファイルがあります :

– 「USBImage.exe」

– 「iRMC_<Firmware-Version>.IMA（iRMC_< ファームウェアバージョン >.IMA）」

➢ USB メモリスティックをコンピュータに接続してください。

➢ 「FTS_<*nnnnnnn*>*.exe*」ファイルもしくは「 USBImag.exe」ファイルを起動してください。

起動したファイルによって、次のどちらかのウィンドウが表示されます。図 .241 を参照してください。

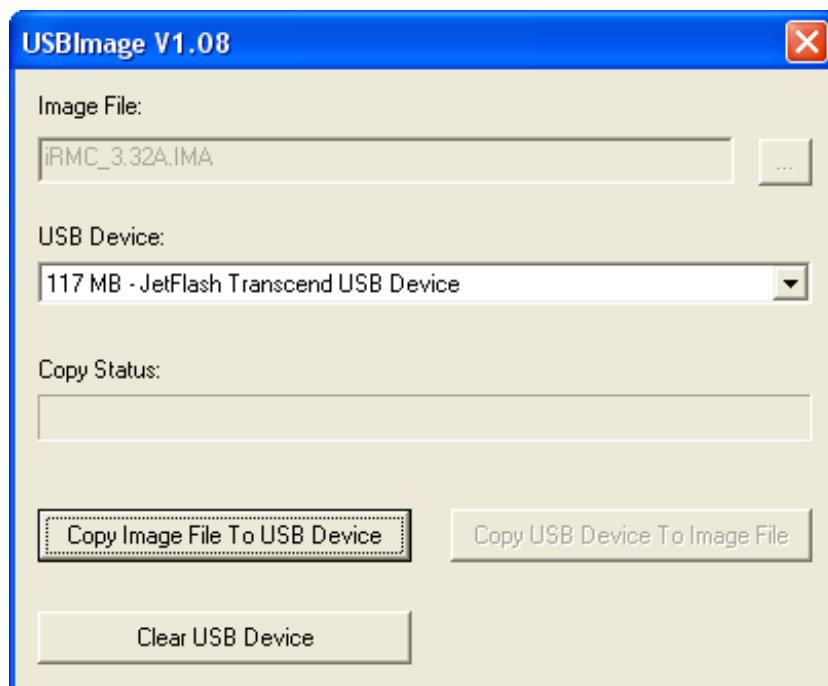



図 .241 :「FTS_<nnnnnnn>.exe」によりイメージファイルを USB メモリスティックにコピー

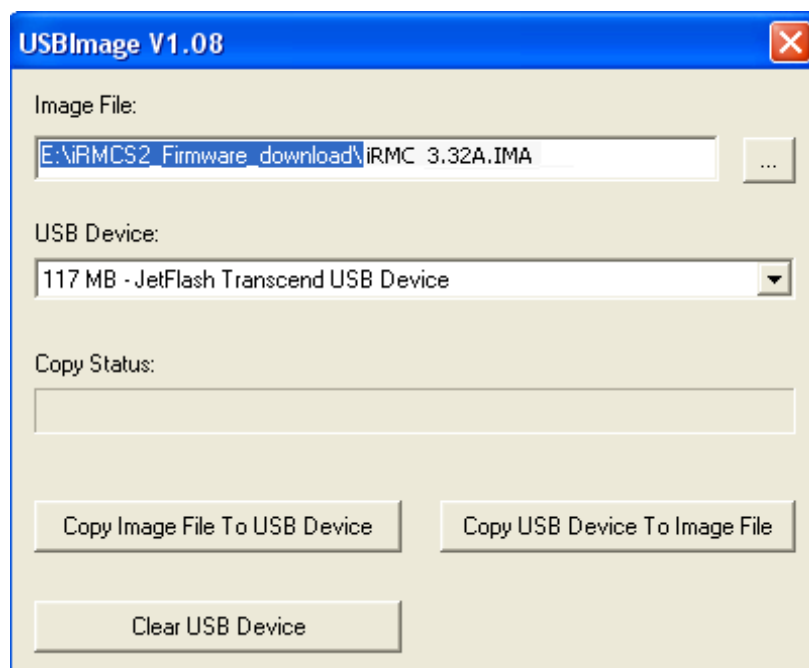



図 .242 :「USBImage.exe」によりイメージファイルを USB メモリスティックにコピー

i 「USBImag.exe」の起動後、「Image File:」下で次のファイルを明示的に指定してください。「iRMC_<Firmware-Version>.IMA」

➤ USB メモリスティックからデータを削除するには「Clear USB Device」を選択してください。

➢「BMC_<Firmware-Version>.IMA」ファイルを USB メモリスティックにコピーし解凍するには「Copy Image File to USB Device」を選択してください。

注意！
この操作は、USB メモリスティックを上書きします。

コピー操作が完了すると、USB メモリスティック上にフラッシュツールおよびイメージファイルが できています。

名前	サイズ	種類	更新日時
FDOS		ファイル フォルダ	2007/08/16 10:44
iRMCldifCreate		ファイル フォルダ	2007/08/13 13:40
MENU		ファイル フォルダ	2007/08/13 13:40
_install.bat	2 KB	Windows バッチ ファイル	2010/02/10 15:24
_SV_BAT	1 KB	Windows バッチ ファイル	2010/02/10 15:24
_vinfo.txt	1 KB	テキスト文書	2010/02/10 15:24
0263284.SDR	256 KB	SDR ファイル	2010/02/10 15:24
boot309A.bin	52 KB	BIN ファイル	2010/02/10 15:24
command.com	65 KB	MS-DOS アプリケーション	2007/02/16 13:29
dcod389A.bin	3,746 KB	BIN ファイル	2010/02/10 15:24
flirmcs2.exe	40 KB	アプリケーション	2010/02/10 15:24
IPMIVIEW.EXE	123 KB	アプリケーション	2010/02/10 15:24
IPMIVIEW.INI	13 KB	構成設定	2010/02/10 15:24
iRMCup.bat	1 KB	Windows バッチ ファイル	2010/02/10 15:24
nommax.ini	1 KB	構成設定	2010/02/10 15:24
readme.txt	1 KB	テキスト文書	2010/02/10 15:24
w32flirmcs2.exe	895 KB	アプリケーション	2010/02/10 15:24
w64flirmcs2.exe	1,034 KB	アプリケーション	2010/02/10 15:24
WAIT.EXE	25 KB	アプリケーション	2010/02/10 15:24
Winflirmcs2.exe	88 KB	アプリケーション	2010/02/10 15:24

図 .243：USB メモリスティック上のイメージファイルおよびフラッシュツール

10.3 ファームウェアイメージのアップデート

iRMC S2 ファームウェアは、iRMC S2 の SRAM メモリで実行されるので、動作中のファームウェアイメージおよび動作していないファームウェアイメージの両方を、オンラインつまりオペレーティングシステムを稼働したままでアップデートできます。

ファームウェアイメージは、次の方法のいずれかでアップデートします。

– iRMC S2 Web インターフェース

– ServerView Update Manager

– ServerView Update Manager Express もしくは ASP

– オペレーティングシステムのフラッシュツール

10.3.1 iRMC S2 Web インターフェースによるアップデート

「*iRMC S2* ファームウェアアップデート」ページは、iRMC S2 のファームウェアイメージがリモート管理端末上もしくは TFTP サーバ上のどちらにあってもアップデートできます。「7.5.5 iRMC S2 ファームウェアのアップデート」（→ P.244）を参照してください。

10.3.2 ServerView Update Manager によるアップデート

ServerView Update Manager では、グラフィカルユーザーインターフェース（Windows）もしくはコマンドラインインターフェース（Windows および Linux）のどちらででも iRMC S2 ファームウェアをアップデートできます。ServerView Update Manager は、「*ServerView Suite DVD 1*」もしくは管理サーバ上のアップデートリポジトリによってアップデートデータにアクセスします。管理サーバのアップデートリポジトリのアップデートは、Download Manager もしくは 「Fujitsu Technology Solutions web server（富士通テクノロジーソリューション Web サーバ）」のダウンロードセクションからの手動ダウンロードで行います。

ServerView Update Manager によるファームウェアアップデートの詳細については、『ServerView Suite - ServerView Update Manager』ユーザーガイドを参照してください。

10.3.3 ServerView Update Manager Express もしくは ASP によるオンライン アップデート

Windows もしくは Linux オペレーティングシステムでは、ServerView Update Manager Express のグラフィカルユーザーインターフェースもしくは ASP（Autonomous Support Package）コマンドインターフェースのどちらででも iRMC ファームウェアをアップデートできます。

Windows では、Windows Explorer から対応する「*ASP-*.exe*」ファイルを選択して ASP を起動することもできます。

Update Manager Express および ASP に関する詳細については、『ServerView Update Manager Express』ユーザーガイドを参照してください。

10.3.4 オペレーティングシステムのフラッシュツールによるアップデート

i　オペレーティングシステムのフラッシュツールによるオンラインアップデートはリカバリフラッシュだけを行い、バージョン確認などは行いません。

稼働しているオペレーティングシステムに応じて、flirmcs2 もしくは WinFLIRMCS2、rFLIRMCS2、sFLIRMCS2 のなかからフラッシュツールを選択してください。

DOS　flirmcs2

Windows:　WinFLIRMCS2

Red Hat Linux:　rFLIRMCS2

SuSE Linux:　sFLIRMCS2（未サポート）

Windows コマンドライン（flirmcs2、WinFLIRMCS2）もしくは Linux CLI（rFLIRMCS2、sFLIRMCS2）からフラッシュツールを起動してください。

コマンド構文とオプションについては「10.5 フラッシュツール」（→ P.448）を参照してください。

必要条件

– 管理対象サーバのファイルシステムに、フラッシュツールとファームウェアアップデートのためのファイルが存在している必要があります。

– 管理対象サーバの Windows もしくは Linux 上で、ServerView エージェントが稼働している必要があります。

次の手順にしたがって処理を行ってください：

次に、USB メモリスティックによるオンラインアップデートについて説明します。「10.2 メモリスティックの設定」（→ P.451）を参照してください。

- 管理対象サーバに USB メモリスティックを接続してください。
- Windows コマンドラインもしくは Linux CLI（Command Line Interface : コマンドラインインターフェース）から、対応する USB メモリスティックのドライブに切り替えてください。
- パラメータ「/s 4」でフラッシュツールを起動して、ファームウェアセレクタの値を 4 に設定してください。

  例えば Windows コマンドラインでは、次のように入力します。
  WinFLIRMCS2 /s 4

- フラッシュツールを対応するアップデートファイルで起動して、ファームウェアのアップデートおよび SDR データのアップデートを開始します。

  例えば Windows コマンドラインでは、次のように入力します。

  WinFLIRMCS2 dcod< ファームウェアバージョン >.bin <nnnnnnn>.sdr /i .

  ファームウェアのアップデート中、進行状況がコンソールに表示されます。エラーが発生した場合、アップデートは中断し、対応するリターンコードが表示されます。（→ P.449）

- 管理対象サーバを再起動します。アップデートされたファームウェアのファームウェアイメージが、自動的に動作します。

10.3.5 FlashDisk メニューによるアップデート

FlashDisk メニューによるアップデートには、再起動可能な USB メモリスティックが必要です。「10.2 USB メモリスティックの設定」(→ P.451)を参照してください。

次の手順にしたがって処理を行ってください。

- 直接もしくはリモートストレージから、管理対象サーバにメモリスティックを接続してください。
- USB メモリスティックから起動します。

再起動完了後、自動的に USB メモリスティック上のデータが RAM ディスクにコピーされます。「*autoexec.bat*」ファイルが自動的に起動します。

FlashDisk メニューが開始されます。

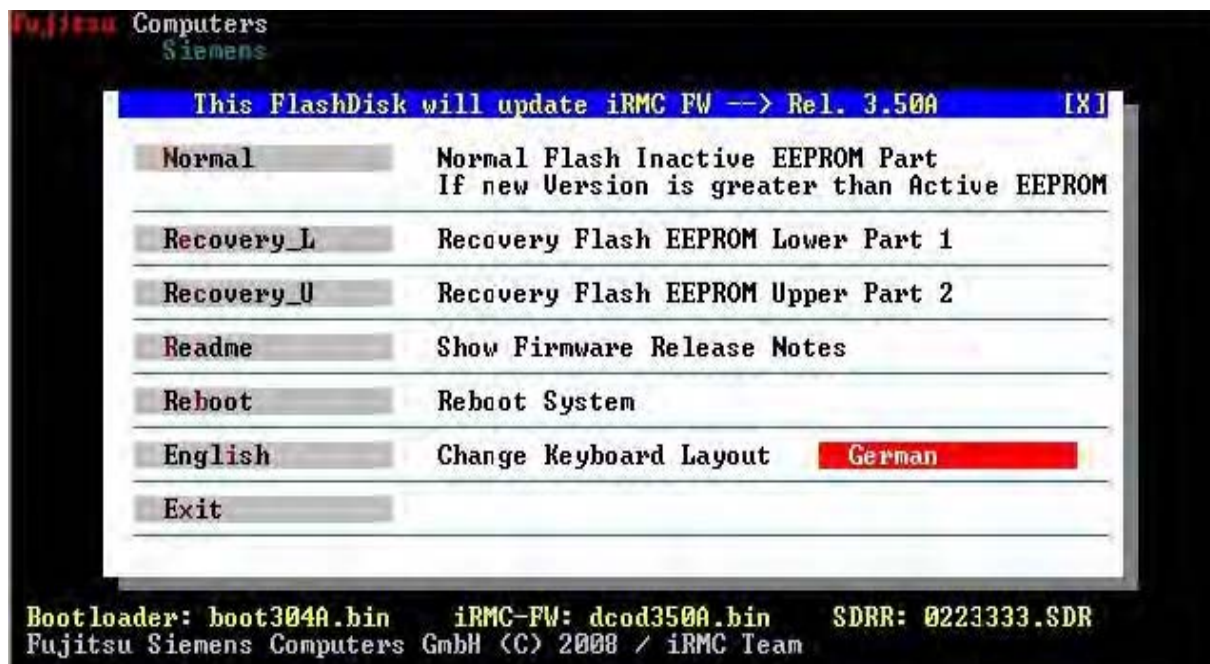



図 .244：FlashDisk メニュー

「*Normal*」

「*normal flash*」を実行します。

ノーマルフラッシュの実行中、両方の EEPROM 領域の状態をみて、動作中のファームウェアが最新版であることを確認します。一方が最新でない場合、すでにアップデートが行われていないかぎり、動作中でないファームウェアの領域がアップデートされます。

「*Recovery _L*」

ファームウェア 1 に対して「*recovery flash*」を実行します。

リカバリフラッシュは、バージョンの確認を一切行わずに、ファームウェア 1 の 3 つの領域すべてに対してフラッシュを実行します。

ファームウェアのダウングレードは、リカバリフラッシュによってのみ可能です。

「*Recovery _U*」

ファームウェア 2 に対して「recovery flash」を実行します。

リカバリフラッシュは、バージョンの確認を一切行わずに、ファームウェア 2 の 3 つの領域すべてに対してフラッシュを実行します。

ファームウェアのダウングレードは、リカバリフラッシュによってのみ可能です。

「*Readme*」

Readme ファイルを開きます。

「*Reboot*」

iRMC S2 がウォームスタートします。

「*English* ／ *German*」

キーボード指定を行います。初期設定値はドイツ語です。

➢ 対応するボタンを選択して、必要なアップデート操作を起動してください

ファームウェアのアップデート中、進行状況がコンソールに表示されます。エラーが発生した場合、アップデートは中断し、対応するリターンコードが表示されます。（→ P.462）

➢ アップデートが完了したら、「*Exit*」を選択して FlashDisk メニューを閉じます。

➢ USB メモリスティックを管理対象サーバから取り外します。

➢ 管理対象サーバを再起動します（たとえば、[Ctrl]+[Alt]+[Del]）。

10.4 エマージェンシーフラッシュ

SDR がシステムと互換でないなどの理由で、iRMC S2 ファームウェアが動作しない場合は、エマージェンシーモードでファームウェアを再起動します。エマージェンシーモードでは、システムが自動的にブートローダにとび、ファームウェアアップデートの準備ができます。

Error LED がエマージェンシーモードであることを示し、識別灯が点灯します。

管理対象サーバを緊急モードにして、iRMC S2 のファームウェアをアップデートするには、次の手順にしたがって処理を行います。

- 電源ユニットのコネクタを切断します。

- コネクタをソケットに再挿入して「Identify key」を押してください。

  これで、管理対象サーバは緊急モードになりました。

- サーバを DOS で再起動し、リカバリフラッシュの手順により iRMC S2 のファームウェアをアップデートします。

ファームウェアが動作中でなければ、再起動には 2 分程度かかります。この間に BIOS が表示する「iRMC S2 Controller Error」というエラーメッセージは無視してください。

10.5 フラッシュツール

WinFLIRMCS2 および rFLIRMCS2、sFLIRMCS2 などのツールと flirmcs2 とは、名前と起動環境だけが異なっています。したがって、flirmcs2 に関する次の説明は、WinFLIRMCS2 および rFLIRMCS2、sFLIRMCS2 にも有効です。「flirmcs2」の部分を、必要に応じて「WinFLRMCS2」もしくは「rFLIRMCS2」、「sFLIRMCS2」と読み替えてください。

構文

flirmcs2 {/v|/o [/4]|/s[< 値 >]}
flirmcs2 {< ファイル 1> [< ファイル 2>] [< ファイル 3>]
　　[/n /l[< ログファイル >] /d /e /4 /i]}
flirmcs2 {/h|/?}

オプション
/v　最新バージョンのコマンドを表示します。
/o　両方のファームウェアのバージョンを表示します。
/s　ファームウェアセレクタの値を表示します。

/s < 値 >
　ファームウェアのリセット後に起動するファームウェアイメージを指定するための値を、ファームウェアセレクタに設定します。
　0　版数が新しいファームウェアをセレクタに設定します。
　1　ファームウェア 1 をセレクタに設定します。
　2　ファームウェア 2 をセレクタに設定します。
　3　版数が古いファームウェアをセレクタに設定します。
　4　書込日が新しいファームウェアをセレクタに設定します。
　5　書込日が古いファームウェアをセレクタに設定します。

< ファイル *1> through* < ファイル *3>*
　アップデートするファイルを 1 ファイル以上指定してください。指定できるのは、次のファイルです。
　「*boot*< ファームウェアバージョン *>.bin*」
　　ブートローダファームウェアをアップデートします。
　「*dcod*< ファームウェアバージョン *>.bin*」
　　ランタイムファームウェアをアップデートします。
　「*<SDR* バージョン *>.SDR*」
　　SDR をアップデートします。

ファームウェアイメージ 2 のアップデートにも、オプション「/4」の設定が必要です（以下を参照してください）。

/4　ファームウェア 2 をアップデートします。

/l [< ログファイル >]
　指定ログファイルにエラーメッセージを出力します。ログファイルを指定しない場合、「flbmc.log」ファイルに出力されます。

/n　コンソールに何も表示しません。
　「/p」および「/d」オプションに優先します。

/np　フラッシュシング操作の間、作業達成率の代わりに回転する棒が表示されます。

/d　追加デバッグ情報を表示します。

/e　エミュレーションモード（デバッグ専用）です。

/i　動作していないファームウェアをアップデートします。

/h および /?
　ヘルプ情報を表示します。

戻り値

0	ファームウェアのアップデートに成功しました。
1	パラメータが正しくないか、指定されていません。
3	PROM タイプは指定できません
4	iRMC S2 と通信できません。
5	バイナリファイルが正しくありません。
8	KCS（Keyboard Control Style interface）アクセスでエラーが発生しました。
9	ターゲット EEPROM との通信がタイムアウトしました。
10	バッファがアロケートされていません。
12	ネットワークノードが使用中です。
13	EEPROM のイレースがタイムアウトしました。
14	EEPROM のフラッシュがタイムアウトしました。
15	EEPROM のイレースでエラーが発生しました。
16	EEPROM のフラッシュでエラーが発生しました。

11 章 iRMC S2 によるオペレーティングシステムのリモートインストール

本章では、ServerView Installation Manager （以下 Installation Manager）および iRMC 機能の「AVR（Advanced Video Redirection : ビデオリダイレクション）」および「リモートストレージ」を使用して、リモート管理端末から管理サーバ上にオペレーティングシステムをインストールする方法を説明しています。

ここでは、次の事項について説明しています。

– リモートストレージメディアによるオペレーティングシステムリモートインストールの基本手順

– ServerView DVD 1（Windows および Linux）によるリモート管理端末からの管理サーバの起動

– リモート管理端末からの管理サーバへの Windows インストール

– リモート管理端末からの管理サーバへの Linux インストール

InstallationManage の機能に関する知識はあることを前提として（『ServerView Suite - ServerView) Installation Manager』を参照してください）、主にリモートストレージメディアの取り扱いについて説明しています。

iRMC S2 によるオペレーティングシステムリモートインストールの必要条件

– iRMC S2 LAN インターフェースが設定されている必要があります。（→ P.32）

– iRMC S2 の「AVR（Advanced Video Redirection : ビデオリダイレクション）」機能および「リモートストレージ」機能を使用するためのライセンスキーがインストールされている必要があります。（→ P.231）

11.1 iRMC S2 によるオペレーティングシステムインストール基本 手順

Installation Manager からみた場合、iRMC S2 によるオペレーティングシステムのリモートインストールは、管理サーバ上でのオペレーティングシステムのローカルな設定およびインストールと同じです。ただ、リモートストレージメディアを利用して、ビデオリダイレクションウィンドウによりリモート管理端末から実行するところが異なります。

Installation Manager によるインストールは、次の手順で行います。

1. 起動に利用したいストレージメディア（DVD 1 もしくは Installation Manager ブートイメージ）をリモートストレージとして接続します。
2. DVD 1 もしくは Installation Manager ブートイメージで管理対象サーバを起動および設定します。
3. リモート管理端末上で Installation Manager を実行し、管理サーバにオペレーティングシステムをインストールします。
4. ビデオリダイレクションウィンドウのマウスポインタを同期します（Linux の場合のみ）。

Windows インストール **CD/DVD** による **Installation Manager** を使用しない **Windows** インストール

リモートストレージでは、Installation Manager もしくは Windows インストール CD ／ DVD のどちら を使っても Windows をリモートインストールできます。リモートストレージメディア操作に関しては、どちらも同じです。

しかし、次のような利点があるため、Installation Manager で Windows インストールを行うべきです。

– Installation Manager 自身が必要なドライバを識別しシステムにコピーします。
– インストール中に Installation Manager のすべての機能を利用できます。たとえば、サーバ管理設定を含む全システムの設定を行えます。

– インストール作業中はマウスカーソルの同期がとれないため、Installation Manager を使用しないインストールにはキーボードが必要です。Installation Manager を利用すれば、すべての設定およびインストール作業がマウスで行えます。

– Installation Manager を使用しないでインストールを行った場合、続いて手動でマウスカーソルの同期作業を行う必要があります。

– Installation Manager によるインストールは、オペレーティングシステム CD/DVD によるインストールと大差のない所要時間でインストールできます。

Linux インストール **CD/DVD** による **Installation Manager** を使用しない **Linux** インストール

システムが必要なドライバが分かっている場合には、Linux インストール CD ／ DVD から Linux インストールを起動できます。

フロッピーディスクのドライバが必要な場合は、インストール作業前に次の手順を行ってください。

－ 起動に使用したいストレージメディア（CD-ROM/DVD-ROM もしくは ISO イメージ）にリモートストレージ接続してください。

– 必要ならば、ストレージメディアからドライバをインストールしてください。

11.2 リモートストレージとしてストレージメディアを接続

リモートストレージを使用して、ネットワーク上の別の場所にある「仮想」ドライブを利用できます。

仮想ドライブのソースとして、次のものが利用できます。

– リモート管理端末上の物理ドライブもしくはイメージファイル。イメージファイルは、ネットワークドライブ上のものでも可（この場合ドライブ名が必要、たとえばドライブ D はドライブ名「D:」）

– リモートストレージサーバをとおしてアクセスするネットワーク上のイメージファイル

> **i** リモートストレージの複数接続 :
>
> 次のどちらかの同時処理が可能です。
>
> – リモート管理端末上の仮想ドライブへの最大 2 つまでのリモートストレージ接続 （AVR Java アプレットで接続されている場合）
>
> もしくは
>
> – 1 台のリモートストレージサーバへの 1 リモートストレージ接続
>
> アプレットによるリモートストレージ接続およびリモートストレージサーバによるリモートストレージ接続を、同時に行うことはできません。

> **i** リモートストレージ接続の状態に関する情報については、iRMC Web インターフェースの「Remote Storage」ページを参照してください。（→ P.354）

リモートストレージの詳細については「6 章 リモートストレージ」（→ P.180）を参照してください。

ストレージメディアをリモートストレージとしてリモートストレージ管理端末へ接続

リモート管理端末上の仮想ドライブから起動を行うために、次のデバイスタイプがサポートされています。

– Floppy ディスク（物理ストレージメディア）

– CD-ROM（物理ストレージメディア）

– DVD-ROM （物理ストレージメディア）

– ISO イメージ（イメージファイル）

– USB メモリスティック（フロッピーをエミュレート）

リモート管理端末上でのリモートストレージへの接続は、次の手順で行ってください。

➢ 「Remote Storage Enabled」許可で、iRMC S2 Web インターフェースにログインしてください。（→ P.210）

➢ 「AVR（Advanced Video Redirection：ビデオリダイレクション）」ページを開いて、AVR を起動してください。（→ P.344）

➢ ビデオリダイレクションウィンドウで「リモートストレージ」を起動してください。（→ P.182）

➢ リモートストレージで使用するストレージメディアを準備してください（→ P.182）。

– Installation Manager でインストールする場合には、ServerView Suite DVD 1 、もしくは Installation Manager 起動イメージおよびオプションでフォーマット済みの USB メモリスティックを準備してください。USB メモリスティックは、ステータスバックアップメディアとして 使用します。

– ベンダーのインストール CD/DVD でインストールする場合には、Windows もしくは Linux インストール CD/DVD およびオプションドライバを準備してください。

i ServerView Suite DVD 1 およびオペレーティングシステムインストール CD/DVD は、いったんイメージファイル (ISO イメージ) としてフォルダに保存してから、リモートストレージとして接続もしくはリモートストレージサーバをとおして接続するべきです。

準備したストレージメディアは、「ストレージデバイス」ダイアログボックスに表示されます。

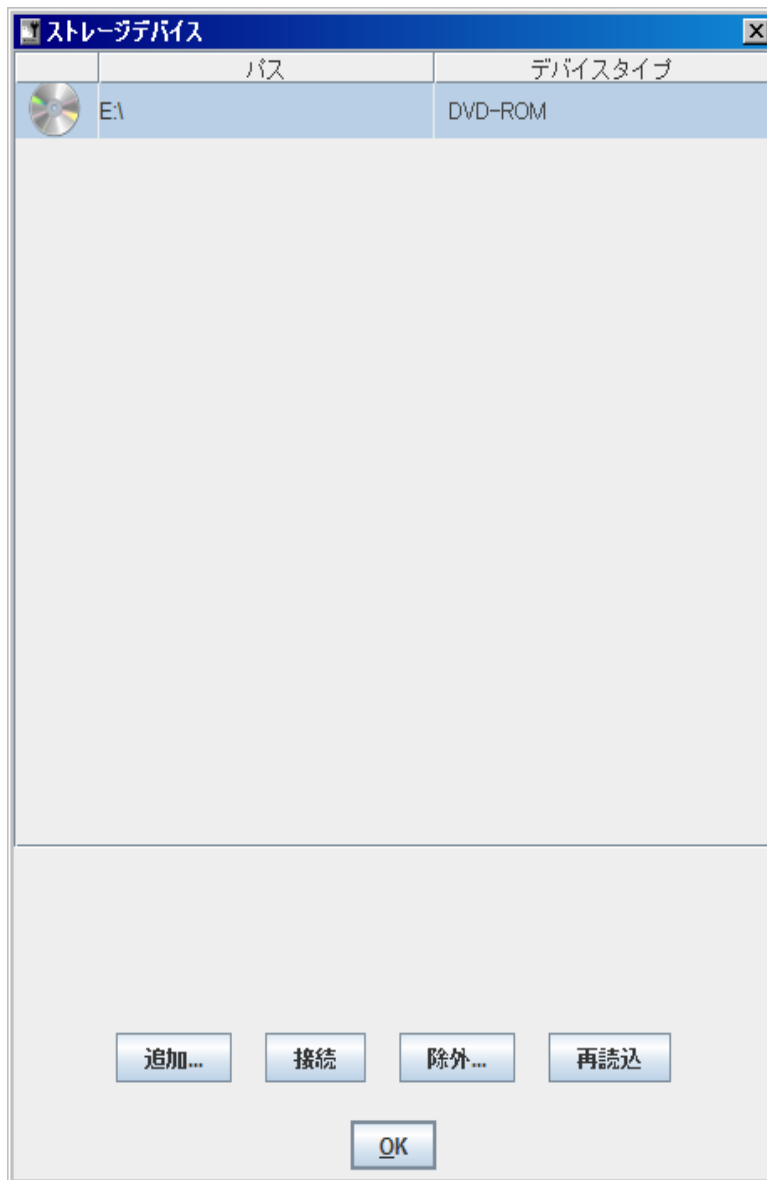



図 .245：ストレージデバイスダイアログボックス：ServerView Suite DVD 1

➢ 接続］を選択して、DVD ROM ドライブ（DVD 1）もしくは Installation Manager ブートイメージにリモートストレージとして接続してください。

リモートストレージサーバの ISO イメージ（イメージファイル）をリモートストレージとして接続

Installation Manager 起動イメージからの起動に、リモートストレージサーバのイメージファイルを使用できます。

i 仮想ドライブがリモートストレージサーバから利用可能になる前に、リモートストレージ サーバをインストールし起動しておく必要があります（「6.2 リモートストレージサーバ を経由するリモートストレージの追加」（→ P.195）を参照してください）。

リモートストレージサーバへの接続は、リモート管理端末から次の手順で行います。

➢「リモートストレージを有効にする」許可で、iRMC S2 Web インターフェースにログインしてください（→ P.210）。

➢「リモートストレージ」ページを選択してください。

➢ リモートストレージサーバに接続してください（→ P355）。

11.3 管理サーバの ServerView Suite DVD 1 からの起動および Installation Manager による設定

リモート管理端末から、次の手順を実行してください。

- iRMC S2 Web インターフェースから、管理対象サーバを起動もしくは再起動してください (→ P.253)。手順は、ビデオリダイレクションウィンドウの起動手順にしたがってください。

  管理対象サーバの BIOS POST フェーズ中、リモートストレージメディアは USB 2.0 デバイスとして表示されます。リモートストレージのストレージメディアは 、BIOS 起動シーケンスに次のエントリとして表示されます（図 .246 を参照してください）。

  – （物理）フロッピーディスクは、別エントリの「FTS RemoteStorage FD-（USB 2.0）」として表示されます。
  – 他のすべてのリモートストレージデバイスタイプは、共有エントリ「CD-ROM DRIVE」と表示されます。

  i ローカル CD-ROM ／ DVD-ROM ドライブおよびリモートストレージとして接続されている CD-ROM/ ／ DVD-ROM ドライブの両方が管理対象サーバにある場合、管理対象サーバはリモートストレージ CD-ROM ／ DVD-ROM ドライブから起動します。

- サーバの起動中は ［F2］を押し続けてください。
- BIOS 設定時は、起動シーケンスが定義可能な「*Boot*」メニューを使用してください。
- 図 .246 にしたがって、起動シーケンスを指定してください。

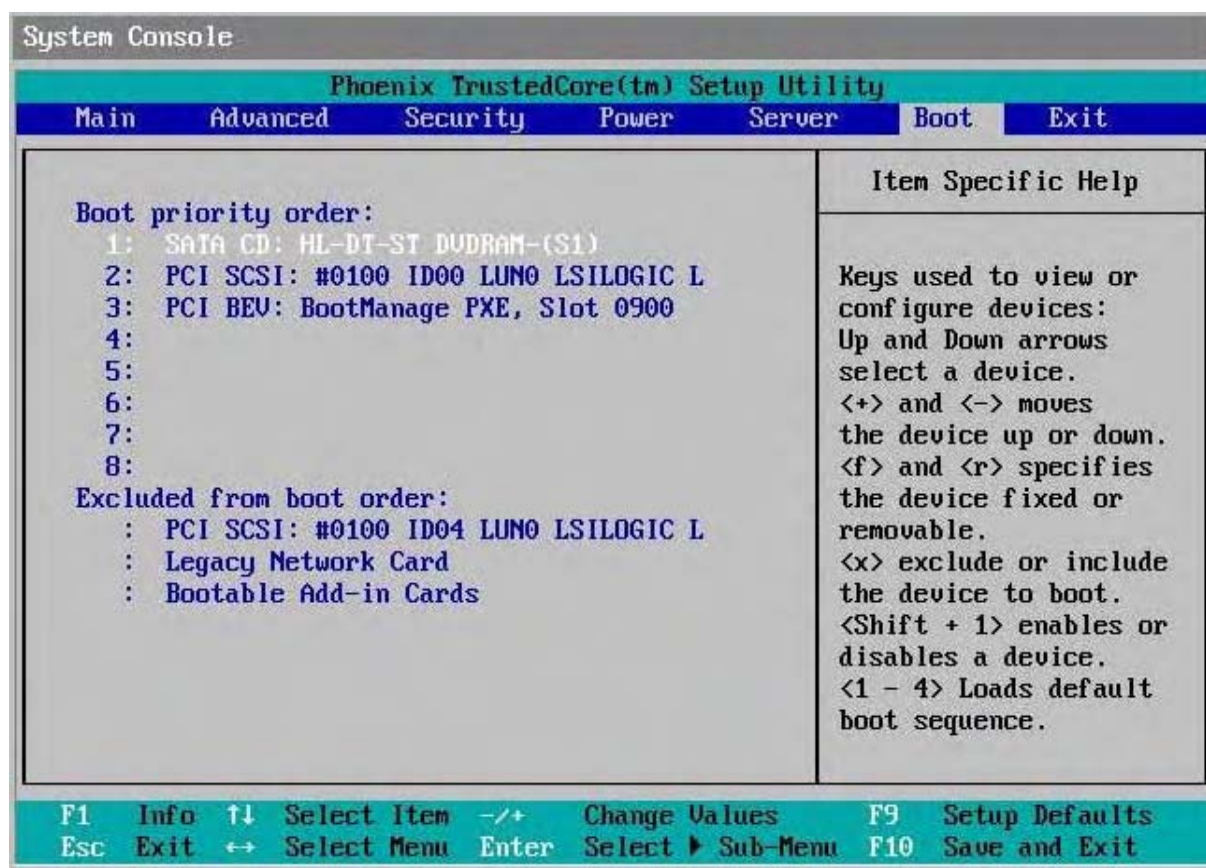



図 .246：BIOS セットアップの起動シーケスメニュー

➢ 設定を保存し、BIOS セットアップを終了してください。

管理対象サーバが、リモートストレージとして接続している ServerView Suite DVD 1 から起動します。

ℹ システムがリモートストレージメディア（**ServerView Suite DVD 1** もしくは **Installation Manager** 起動メージ）から起動しない場合は、次の手順を実行してください。

➢ BIOS POST フェーズ中にストレージメディアが表示されているかを確認し、必要ならばストレージメディアをリモートストレージとして接続してください。

➢ 指定した起動シーケンスが正しいかどうかを確認してください。

リモートストレージメディアの ServerView Suite DVD 1 からの起動には、5 分程度かかります。起動中は、次のウィンドウが表示されます。

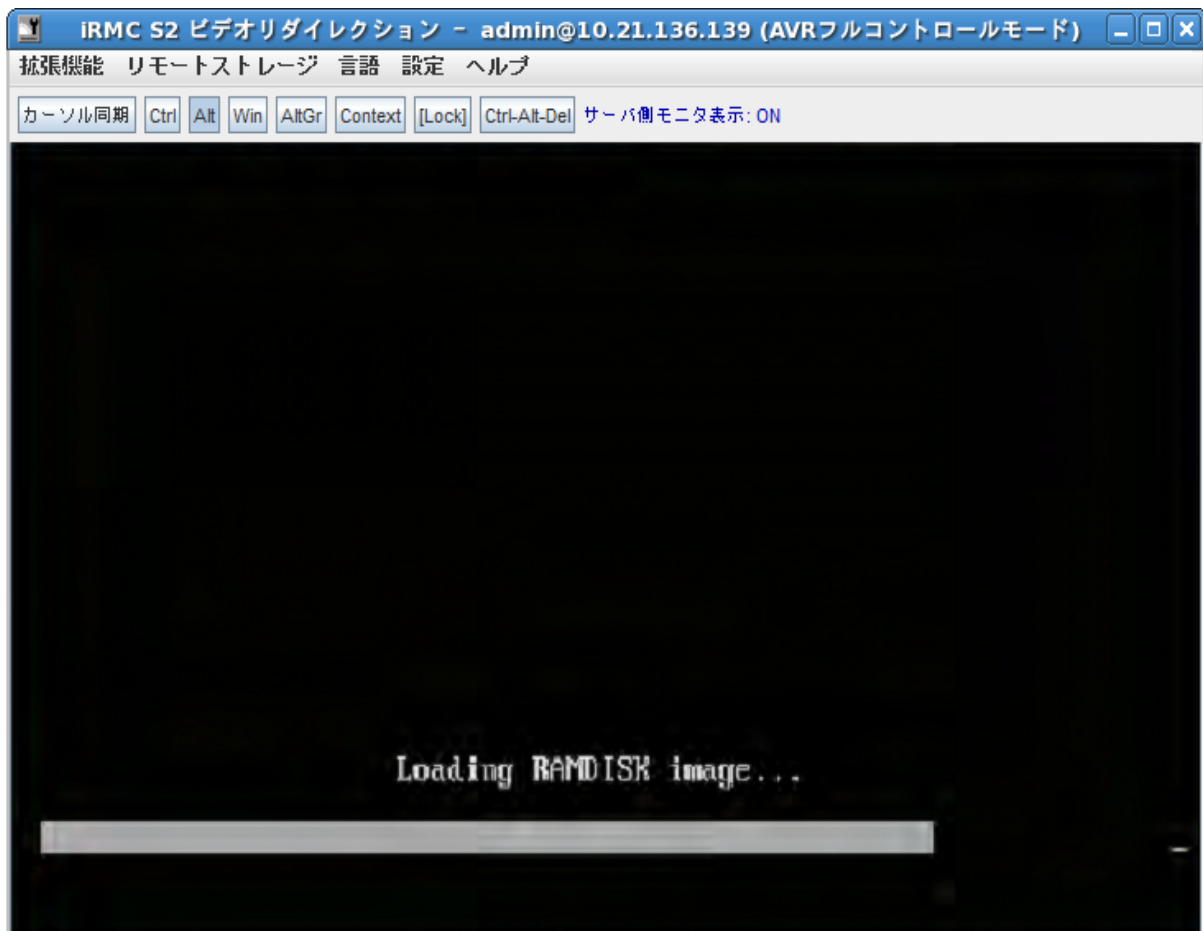



図 .247：ServerView Suite DVD 1 で起動された管理対象サーバ

起動完了時に表示されるダイアログボックスで、ステータスバックアップ領域（ステータスバックアップメディア）を指定してください（図 .248 を参照してください）。

オペレーティングシステムをインストールする前に、リモート管理端末のリダイレクトウィンドウで、ローカルなマウスカーソルおよび管理対象サーバのカーソルを同期します（ 図 .248 を参照してください）。リダイレクトウィンドウでのマウスカーソルの同期に関する詳細については「5.2.4.1 マウスポインタの同期」（→ P.164）を参照してください。

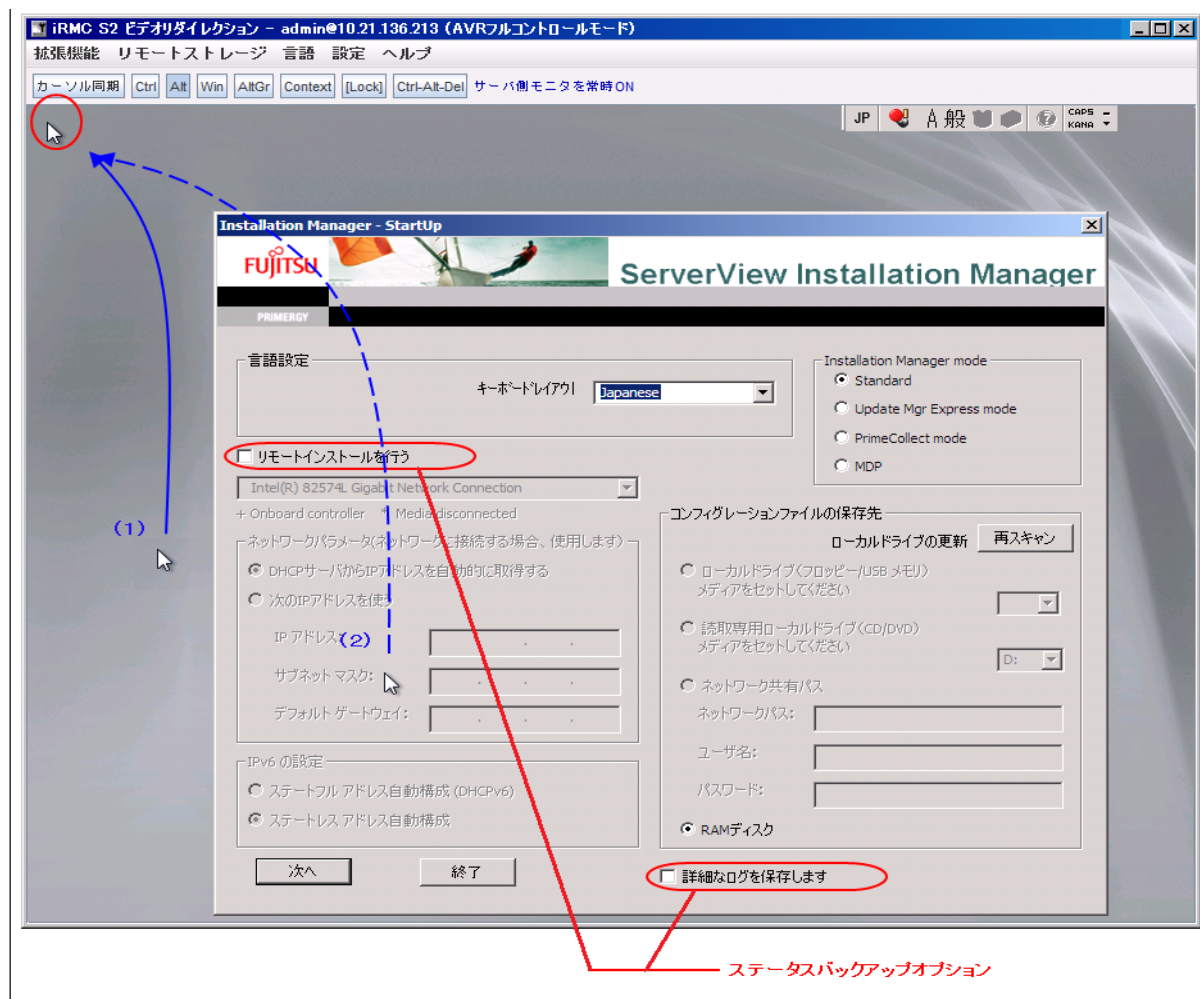



図 .248：Installation Manager：ステータスバックアップメディアの選択

–「Installation Manager mode」で「Standard mode」を選択してください。

➢ 設定データをローカルな交換可能データメディアもしくはネットワークメディアのどちらに保存するかを指定してください。

ステータスバックアップオプションを選択しないで再起動すると、設定データがすべて失われるので注意してください。

「*Status backup medium*」

バックアップメディアを「write-protected」にしないでください。

システムの起動時には､USB スティックが USB ポートに接続されている必 要があります。これを忘れた場合に、設定ファイルを保存するには、

すぐに USB スティックを接続して、ServerView Suite DVD 1 で再起動してください。

- 「local drive (floppy ／ USB stick)」オプションを選択してください。

- ボックスで、このオプションに対応した正しいドライブを選択してください。

Installation Manager ステータスディスク作成に関する詳細については､『ServerView Suite - ServerView Installation Manager』を参照してください。

「*Connecting the status medium and/or the installation media via the network*」

- 必要な共有を設定してください。

事前設定したファイルメディアおよび／もしくはネットワーク使用可能 なインストールメディアを作成する場合は、必ずこのオプションを選択してください。最新の Installation Manager セッションでは、使用中のイン フラに応じて、DHCP によるテンポラリな IP アドレスと手動で設定する IPv4 もしくは IPv6 アドレスのどちらかを使用できます。

- ［次へ］を選択して Installation Manager を起動してください。

ローカルディプロイメントの開始

Installation Manager を起動すると Welcome 画面が表示されます。

図 .249：Installation Manager - Welcome 画面

➤［*Deployment*］を指定して、ローカルインストール（ディプロイメント）を開始してください。

インストールの準備として、Installation Manager ウィザードにしたがい、システム設定およびそれに続くオペレーティングシステムの自動インストールに必要な情報を設定します。

管理対象サーバのローカル CD ROM ／ DVD ROM ドライブをインストールソースとして設定します。また、Windows installation CD ／ DVD をリモートストレージとして 管理対象サーバに接続する場合には、それがリモート管理端末の CD ROM ／ DVD ROM ドライブで利用できるようにします。（「11.4.1 設定に続く管理対象サーバ Windows インストール」（→ P.464）を参照してください）。

Installation Manager による設定が完了すると、Windows インストール（→ P.464）もしくは Linux インストール（→ P.481）の「インストール情報」ダイアログページが表示されます。ここから、インストールを開始します。

11.4 管理対象サーバへのオペレーティングシステムインストール

設定完了後、管理対象サーバにオペレーティングシステムをインストールします。

11.4.1 管理対象サーバ への Windows インストール

設定完了後、Installation Manager は次のダイアログページを表示します。

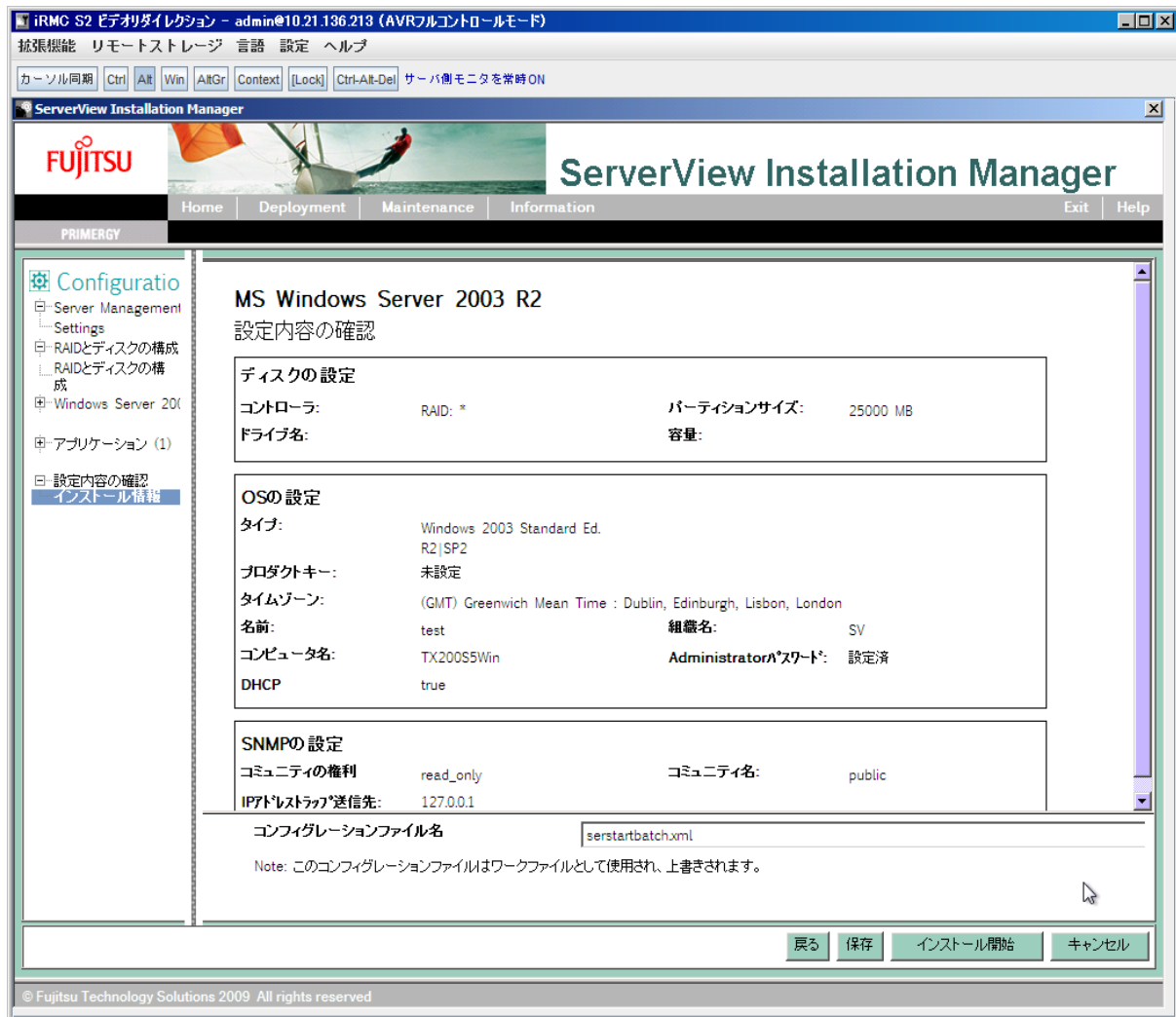



図 .250 : Installation Manager – インストール開始

管理対象サーバのローカル CD ROM/DVD ROM ドライブをインストール元として設定し、リモート管理端末で次の手順を行なってください。

➢ 動作中のリモートストレージ接続を切断してください（→ P.193）。

➢ リモート管理端末の DVD ROM ドライブから ServerView Suite DVD 1 を取り外してください。

➢ この DVD ROM ドライブに Windows インストール CD/DVD を挿入してください。

i 「autostart」が動作中の場合は、クローズしてください。

➢ Windows インストールが入っている CD ROM/DVD ROM ドライブをリモートストレージとして接続してください（→ P.189）。

➢ ［インストール開始］を選択してください。

すべてのインストールファイルが、管理対象サーバにコピーされます。

コピーが完了すると、Installation Manager が確認ダイアログページを表示し、管理対象サーバを再起動する前に取り外し可能なすべてのストレージメディアをドライブから取り外すように指示します。

i 特にリモートストレージ接続は、システムを再起動する前に遮断する必要があります。

➢ システムを再起動する前に、リモートストレージ接続を遮断してください。この手順は、次のとおりです。

➢ 「リモートストレージ」を起動してください（→ P.182）

接続されているストレージデバイスおよび「安全な取り外し」のための注意が、「ストレージデバイス」ダイアログボックスに表示されます。図 .251 を参照してください。

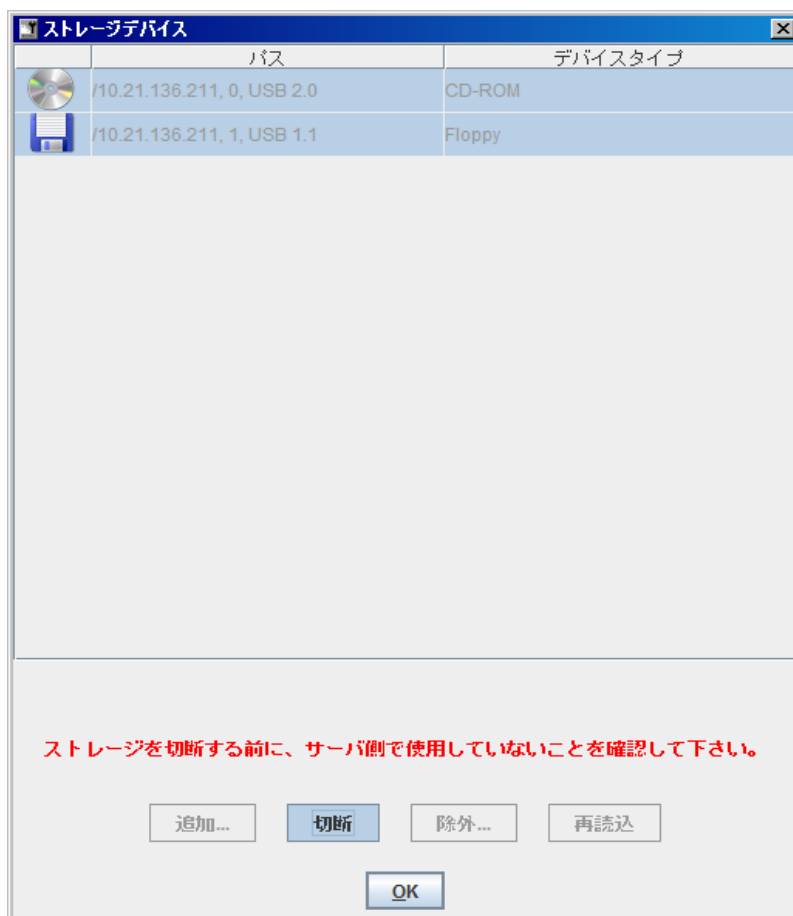



図 .251：ストレージデバイスダイアログボックス：リモートストレージ切断

- アプリケーションおよびプログラムがアクセスしていないことを確認して、ストレージデバ スを安全に取り外してください。
- ［*切断*］を選択して、すべてのリモートストレージ接続を解除してください。

➢ 確認ダイアログページで［*OK*］を選択して、管理対象サーバを再起動してください。

管理対象サーバの再起動完了後、AVR からすべてのインストールを監視できます。図 .252 を参照してください。

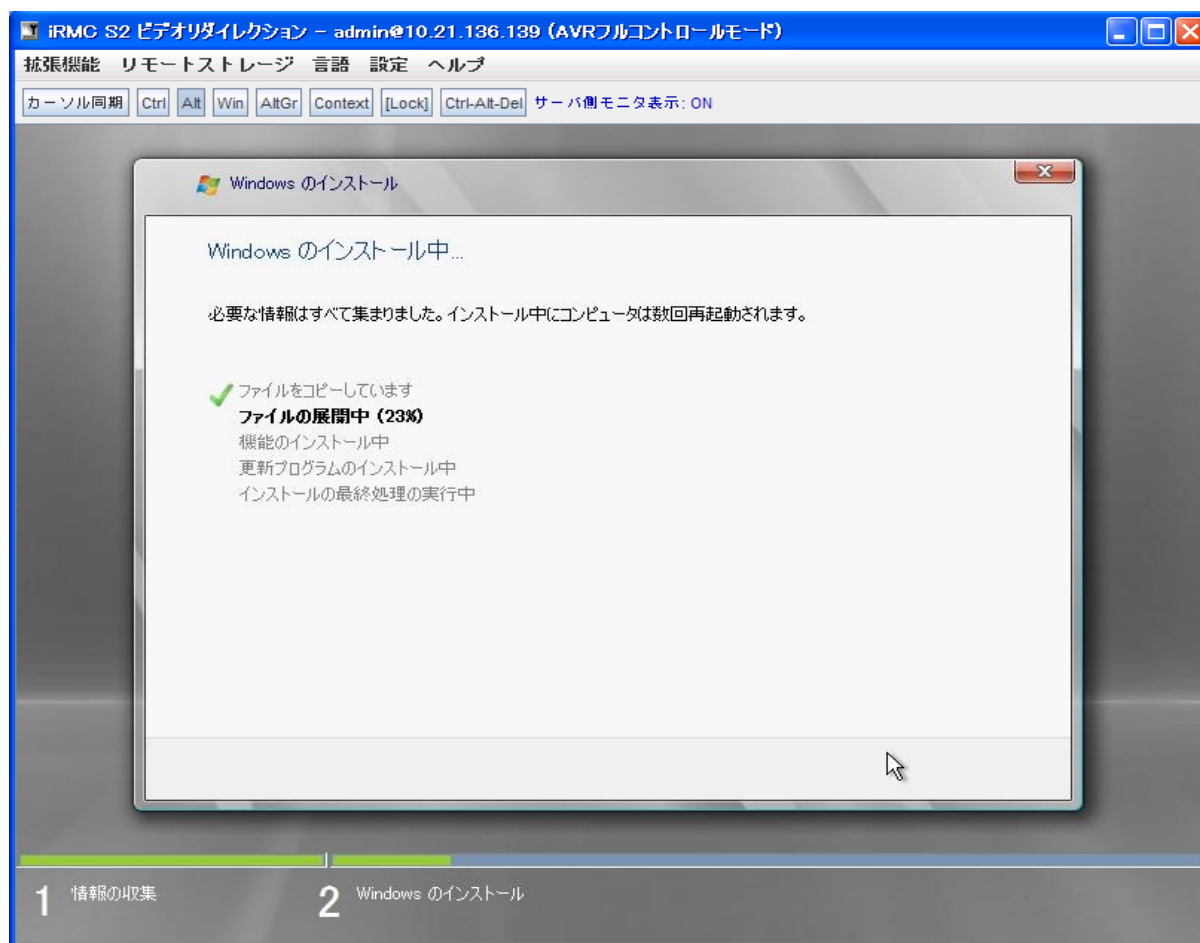



図 .252 : リダイレクションウィンドウでの Windows インストールのモニタリング

i Windows インストール CD/DVD により Windows をインストールする場合は、

オペレーティングシステムのインストール完了後に管理対象サーバ上で次の設定を行い、マウスカーソルを確実に同期する必要があります。

– マウスポインタの速度

– ハードウェア加速

この設定に関する詳細については、「5.2.4.2 管理対象 Windows サーバ : マウスポインタ同期設定の調整」(→ P.166) を参照してください。

Installation Manager で Windows をインストールする場合は、問題のないマウスポインタ同期操作が自動的に行われます。

12 IPMI OEM コマンド

本章では、iRMC S2 がサポートする OEM 特有の IPMI コマンドの選択について説明します。

12.1 概要

iRMC S2 では以下の OEM 特有の IPMI コマンドをサポートします。

- **SCCI** 準拠の自動電源投入／電源遮断コマンド

  （SCCI：**S**erverView **C**ommon **C**ommand **I**nterface（ServerView 共通コマンドインターフェース））

  – 0115 Get Power On Source

  – 0116 Get Power Off Source

  – 011C Set Power Off Inhibit

  – 011D Get Power Off Inhibit

  – 0120 Set Next Power On Time

- **SCCI** 準拠の通信コマンド

  – 0205 System OS Shutdown Request

  – 0206 System OS Shutdown Request and Reset

  – 0208 Agent Connect Status

  – 0209 Shutdown Request Cancelled

- **SCCI** 準拠のシグナリングコマンド

  – 1002 Write to System Display

- ファームウェア特有のコマンド

  – 2004 Set Firmware Selector

  – 2005 Get Firmware Selector

  – C019 Get Remote Storage Connection or Status

  – C01A Set Video Display On/Off

- **BIOS** 特有のコマンド
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC S2** 特有のコマンド
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F543 Get SEL entry long text
  - F545 Get SEL Entry Text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Reset Nonvolatile Cfg Variables to Default
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

12.2 IPMI OEM コマンドの記述

この節では、個別の OEM 特有の IPMI コマンドについて説明します。

12.2.1 記述形式

本章で記載する OEM 特有の IPMI コマンドは、IPMI コマンドを記述するための IPMI 標準で使用する形式によって記述されます。

IPMI 標準では、各コマンドに対する入力パラメータと出力パラメータを一覧にしたコマンド表を使用して IPMI コマンドを記述します。

IPMI 標準の情報については以下のサイトを参照してください。

http://developer.intel.com/design/servers/ipmi/index.htm

12.2.2 SCCI 準拠の自動電源投入／遮断コマンド

01 15 - Get Power On Source

本コマンドは最後に行われた自動電源投入の理由を返します。理由には以下にあげるものがあります。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**01** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**16** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	3	**01** データ長
	4	電源遮断原因：最後の自動電源遮断の理由

電源投入原因	説明
0x00	ソフトウェアまたはコマンド
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	電源障害後の自動再起動
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害によるシャットダウン後の自動再起動
0x05	臨界温度によるシャットダウン後の自動再起動
0x08	ウォッチドックタイムアウト後の再起動
0x09	リモートオン（モデム RI ライン、SCSI ターミネーションパワー、LAN、IC カードリーダー・・・）
0x0C	CPU エラー後の再起動
0x15	ハードウェアリセットによる再起動
0x16	ウォームスタート後の再起動
0x1A	PCI バス電源管理イベントによる電源投入
0x1D	Telnet/SSL 経由のリモート制御による電源投入
0x1E	Telnet/SSL 経由のリモート制御による再起動／リセット

01 16 - Get Power Off Source

本コマンドは最後に行われた自動電源遮断の理由を返します。理由にはは以下にあげるものがあります。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**01** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**16** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	3	**01** データ長
	4	電源遮断原因：最後の自動電源遮断の理由

電源投入原因	説明
0x00	ソフトウェア（SWOFF、コマンドによる電源遮断）
0x01	電源スイッチ（フロントパネルまたはキーボード上）
0x02	AC 電源障害
0x03	クロックまたはタイマー（ハードウェア RTC またはソフトウェアタイマー）
0x04	ファン障害
0x05	臨界温度
0x08	ウォッチドックタイムアウト繰り返し後の電源遮断
0x0C	CPU エラー繰り返し後の電源遮断
0x1D	Telnet/SSL 経由のリモート制御による電源遮断

01 1C - Set Power Off Inhibit

本コマンドは電源遮断防止フラグを設定します。この設定により、正当な理由なくサーバの電源をオフにしようとした場合に一時的に電源遮断が防止されます。

電源遮断防止フラグが設定されていると、サーバの「Power Off」、「Power Cycle」または再起動を実行しようとした理由がファームウェアによって保存されますが、動作は実行されません。最後に実行したサーバの「Power Off」、「Power Cycle」または再起動の理由が常時保存されます。

保存された動作は電源遮断防止フラグをリセットしたときのみ実行されます。電源遮断防止フラグは、電源障害後、またはリセットボタンの押下時に自動的にリセットされます。電源遮断防止フラグには、メインメモリダンプを作成する際に使用するダンプフラグと同じ効果があります。この場合、ダンプを作成する前にイニシエーターで必ずフラグを設定し、ダンプが完了したときにリセットします。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**01** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**1C** コマンド指定子
	5	**00** オブジェクト ID
	6.7	**00 00** 値 ID
	8	**01** データ長
	9	電源遮断防止フラグ：0 ＝ 防止しない、1 ＝ 防止する
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2.4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

01 1D - Get Power Off Inhibit

本コマンドは電源遮断防止フラ

*電源遮断防止フラグ*の詳細については、474 ページの「01 1C - Set Power Off Inhibit」の説明を参照してください。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**01** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**1D** コマンド指定子
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**01** 応答データ長
	6	電源遮断防止フラグ：0 ＝防止しない、1 ＝防止する

01 20 - Set Next Power On Time

本コマンドは、設定スペースに保存されている電源投入／遮断時刻とは別に所定の時間でシステムの電源を投入します。

コマンドは 1 回のみ有効です。

前回 01 20 コマンドで設定した「電源投入」時刻をキャンセルするには、次の 01 20 コマンドで「0」を「電源投入」時刻に指定します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**01** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**20** コマンド指定子
	5	**00** オブジェクト ID
	6.7	**00 00** 値 ID
	8	**04** データ長
	9.12	時刻（LSB ファースト）（下記参照）
応答データ	-	**BC**
	-	**01**
	1	完了コード
	2.4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

時刻（LSB ファースト）

システムの電源を再度投入した時刻（UNIX 特有の形式）です。時刻は不揮発メモリに保存されません。設定単位は 1 分毎です。システムの電源を投入した後、内部で時刻が 0 に 設定されます。

Time == 0 の場合、システムの電源は投入されません。

12.2.3 SCCI 準拠の通信コマンド

SCCI 準拠の通信コマンドには、エージェントサービスが OS で起動していることが必要です。コマンドを実行するには、iRMC S2 が最終的に動作を行うエージェントと通信します。

02 05 - System OS Shutdown Request

本コマンドはサーバのオペレーティングシステムのシャットダウンを開始します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**02** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**05** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

02 06 - System OS Shutdown Request and Reset

本コマンドはサーバのオペレーティングシステムのシャットダウンを開始した後にシステムを再起動します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**02** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**06** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

02 08 - Agent Connect Status

本コマンドはエージェントがアクティブであるかどうかを確認します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**02** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**08** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	**01** データ長
	6	接続状態： 00 ＝接続が切断された、エージェントが接続されていない 01 ＝接続が再確立された、エージェントが接続されている

02 09 Shutdown Request Cancelled

本コマンドは発行されたシャットダウン要求をキャンセルします。

要求データ		**B8** NetFnlLUN：OEM ／グループ
	-	**02** Cmd：コマンドグループコミュニケーション
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**09** コマンド指定子
応答データ	-	**BC**
	-	**02**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.2.4 SCCI 準拠のシグナリングコマンド

10 02 - Write to System Display

本コマンドは、LocalView ディスプレイ（接続されている場合）に文字を書き込むために使用します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**10** Cmd：コマンドグループファンテスト
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**02** コマンド指定子
	5	オブジェクトインデックス：：書き込みを行うディスプレイの線
	6.7	値 **ID**（未使用）
	8	長さ 1 ずつ増加する書き込む文字数（文字列がヌル終端である必要はありません。ディスプレイの長さを超える文字列は切り捨てます。）
	9	属性 0 ＝文字列を左詰めで書き込みます。 1 ＝文字列を右詰めで書き込みます。
	10:10+n	ディスプレイに書き込む文字（文字列がヌル終端である必要はありません。）
応答データ	-	**BC**
	-	**10**
	1	完了コード
	2.4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

12.2.5 Firmware 特有のコマンド

20 04 - Set Firmware Selector

本コマンドは、ファームウェアのリセット後にアクティブになる IRMC S2 のファームウェアイメージを設定します。

要求データ	-	**20** NetFnlLUN：ファームウェア
	-	**04** CMD：コマンドグループファームウェア
	1	セレクタ： 0 ＝ Auto（版数が新しいファームウェアを選択します。） 1 ＝ Low Firmware Image 2 ＝ High Firmware Image 3 ＝ Auto oldest version（版数が古いファームウェアを選択します。） 4 ＝ MRP（書込日が新しいファームウェアを選択します。） 5 ＝ LRP（書込日が古いファームウェアを選択します。）
応答データ	-	**24**
	-	**04**
	1	完了コード

20 05 - Get Firmware Selector

本コマンドは現在のファームウェアセレクタ設定を返します。

要求データ	-	**20** NetFnlLUN：ファームウェア
	-	**05** CMD：コマンドグループファームウェア
応答データ	-	**24**
	-	**05**
	1	完了コード
	2	次回のブートセレクタ： 0 ＝ Auto（最新のファームウェアバージョンの EEPROM を選択します。） 1 ＝ Low EEPROM 2 ＝ High EEPROM 3 ＝ Auto oldest version（最も古いファームウェアバージョンの EEPROM を選択します。） 4 ＝ MRP（最後に更新したファームウェアを選択します。） 5 ＝ LRP（最初に更新したファームウェアを選択します。）
	3	動作中のセレクタ：どのファームウェアが現在動作中であるかを示します。 1 ＝ Low EEPROM 2 ＝ High EEPROM

C0 19 - Get Remote Storage Connection or Status

本コマンドは、渡されたパラメータに応じて、以下に関する情報を返します。

– 使用できるリモートストレージ接続があるか

– リモートストレージ接続の状態および種類

要求データ 1 が「1」に設定された場合、コマンドはストレージメディアがリモートストレージとして接続されているかどうかの情報を返します。

要求データ	-	**C0** NetFnlLUN：OEM
	-	**19** CMD：コマンドグループファームウェア
	1	01
	2	00
	3	00
応答データ	-	**C4**
	-	**19**
	1	完了コード
	2	**01**
	3	**00**：未接続 **01**：接続されている
	4	**00**
	5	**00**

要求データ 1 が「2」に設定された場合、コマンドは任意のリモートストレージ接続の状態および種類に関する情報を返します。

要求データ	-	**C0** NetFnlLUN：OEM
	-	**19** CMD：コマンドグループファームウェア
	1	02
	2	00
	3	00 ＝接続 0 01 ＝接続 2
応答データ	-	**C4**
	-	**19**
	1	完了コード
	2	**02**
	3	**00**
	4	**00**
	5	**00** ＝無効／未知 **01** ＝アイドル **03** ＝接続済み **04**＝接続再試行に失敗または試行回数の終了 **05**＝接続切断 **06** ＝切断中
	6	**00** ＝無効／未知 **01** ＝ストレージサーバ／ **IPMI** **02** ＝アプレット **03** ＝なし／未接続

C0 1A - Set Video Display On/Off

本コマンドは、ローカルコンソールの有効／無効を切り替えることができます。

要求データ	-	**C0** NetFnlLUN：OEM
	-	**1A** Cmd：コマンドグループファンテスト
	1	00 ＝ビデオ表示を有効に設定します。 01 ＝ビデオ表示を無効に設定します。
応答データ	-	**C4**
	-	**1A**
	1	完了コード

12.2.6 BIOS 特有のコマンド

F1 09 - Get BIOS POST State

本コマンドは BIOS が POST 中であるかどうかの情報を提供します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F1** Cmd：コマンドグループ BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**09** コマンド指定子
応答データ	-	**BC**
	-	**F1**
	1	完了コード
	2.4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	[7:1] – 予備 [0] – BIOS POST 状態： 0 ＝ BIOS が POST 状態ではありません。 1 ＝ BIOS が POST 状態です。

F1 15 - Get CPU Info

本コマンドは CPU 内部情報を返します。iRMC S2 では、POST フェーズ中に BIOS から本情報を取得します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F1** Cmd：コマンドグループ BIOS
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**15** コマンド指定子
	5	CPU のソケット番号（0 ベース）
応答データ	-	**BC**
	-	**F1**
	1	完了コード： 01 ＝未実装の CPU ソケット
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	CPU ID、LSB ファースト
	7	プラットフォーム ID
	8	ブランド ID
	9:10	CPU の最大コアスピード [MHz]、LSB ファースト
	11:12	Intel QuickPath インターコネクト [MT/s]、LSB ファースト
	13	熱制御オフセット
	14	熱ダイオードオフセット
	15	CPU データ予備
	16:17	記録 ID CPU 情報 SDR、LSB ファースト
	18:19	記録 ID CPU ファン制御 SDR、LSB ファースト
	20:21	CPU ID ハイワード、LSB ファースト（なければ o）

12.2.7 iRMC S2 特有のコマンド

F5 10 - Get System Status

本コマンドは、電源状態、エラー状態等のシステムの各種内部情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループメモリ
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**10** コマンド指定子
	5	タイムスタンプ
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	システム状態（詳細については下記を参照してください。）
	6	シグナリング（詳細については下記を参照してください。）
	7	通知（詳細については下記を参照してください。）
	8	**POST** コード

i タイムスタンプは、通知バイトの評価のみに適用されます。

システム状態

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

シグナリング

Bit 7 - Localize LED

Bit 6 -

Bit 5 -

Bit 4 -

Bit 3 - CSS LED

Bit 2 - CSS LED

Bit 1 - Global Error LED

Bit 0 - Global Error LED

通知

Bit 7 - SEL Modified (New SEL Entry)

Bit 6 - SEL Modified (SEL Cleared)

Bit 5 - SDR Modified

Bit 4 - Nonvolatile IPMI Variable Modified

Bit 3 - ConfigSpace Modified

Bit 2 -

Bit 1 -

Bit 0 - New Output on LocalView display

F5 12 - Get EEPROM Version Info

本コマンドは、EEPROM に保存されている現在のバージョン（bootloader、ファームウェアおよび ADR）に関する情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ	
	-	**F5** Cmd：コマンドグループメモリ	
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト	
	4	**12** コマンド指定子	
	5	EEPROM# 00 ＝ EEPROM 1、01 ＝ EEPROM 2	
応答データ	-	BC	
	-	F5	
	1	完了コード	
	2:4	80 28 00 IANA-Enterprise-Number FTS、LSB ファースト	
	5	状態 00 ＝チェックサムエラーランタイム FW、01 ＝ OK	
	6	メジャー FW リビジョン	バイナリコード
	7	マイナー FW リビジョン	BCD コード
	8:10	Aux FW リビジョン	バイナリコード（メジャー／マイナー／ Aux）
	11	メジャー FW リビジョン	ASCII コード
	12	メジャー SDRR リビジョン	BCD コード
	13	マイナー SDRR リビジョン	BCD コード
	14	SDRR リビジョン文字	ASCII コード
	15	SDRR-ID	LSB バイナリコード
	16	SDRR-ID	MSB バイナリコード
	17	メジャー Booter リビジョン	バイナリコード
	18	メジャー Booter リビジョン	BCD コード
	19:20	Aux Booter リビジョン	バイナリコード（メジャー／マイナー）

F5 43 - Get SEL entry long text

本コマンドは任意の SEL エントリをロングテキストに変換します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ iRMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**43** コマンド指定子
	5:6	SEL レコードのレコード ID 、LSB ファースト 0x0000：最初のレコードを取得します。 0xFFFF : 最後のレコードを取得します。
	7	応答 SLE テキストのオフセット
	8	**MaxResponseData Size** 応答の変換済み **SLE** データサイズ（16:n）
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5:6	次のレコード **ID**
	7:8	実際の **ID**
	9	レコードタイプ
	10:13	タイムスタンプ
	14	重大度： Bit 7： 0 = CSS コンポーネントなし 1 = CSS コンポーネントあり Bit 6-4： 000 = INFORMAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown' Bit 3-0： 予備、0000 とします。
	15	テキスト全体のデータ長
	16:n	変換済み **SEL** データ 要求部分 (n=16+ MaxResposDataSize - 1)
	n+1	文字列終了 「\0」という文字をつけます。

F5 45 - Get SEL Entry Text

本コマンドは任意のシステムイベントログ SEL エントリを ASCII テキストに変換します。

要求データ

-	**B8** NetFnlLUN：OEM ／グループ
-	**F5** Cmd：コマンドグループ iRMC
1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
4	**45** コマンド指定子
5:6	SDR のレコード **ID**、LSB ファースト

応答データ

-	**BC**
-	**F5**
1	完了コード
2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
5:6	次のレコード **ID**
7:8	実際の **ID**
9	レコードタイプ
10:13	タイムスタンプ
14	重大度： Bit 7： 0 ＝ CSS コンポーネントなし 1 ＝ CSS コンポーネントあり Bit 6-4： 000 ＝ INFORMAL 001 = MINOR 010 = MAJOR 011 = CRITICAL 1xx = Unknown' Bit 3-0： 予備、0000 とします。
15	データ長
16:35	変換済み **SEL** データ

F5 B0 - Set Identify LED

本コマンドにより、サーバオン／オフの識別灯（青色）を切り替えることが可能です。さらに、識別灯に直接接続された GPIO の設定および読み込みが可能になります。

サーバ上の識別切り替えを使用して識別灯を切り替えることも可能です。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B0** コマンド指定子
	5	識別灯： 0 ＝識別灯オフ 1 ＝識別灯オン
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 B1 - Get Identify LED

本コマンドは、サーバの識別灯（青色）の状態に関する情報を返します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**B1** コマンド指定子
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	5	識別灯の状態（ビット 0 のみが該当します。）

F5 B3 - Get Error LED

本コマンドは、サーバの Error LED（赤色）および CSS LED（黄色）の状態に関する情報を返します。Error LED はコンポーネントの最も重大なエラー状態を示します。CSS LED は、ユーザー自身が障害を修復できるかどうかを示します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ **BMC**
	1:3	**80 28 00**　IANA-Enterprise-Number FTS、LSB ファースト
	4	**B3** コマンド指定子
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00**　IANA-Enterprise-Number FTS、LSB ファースト
	5	**Error LED の状態：** 0 ＝ CSS off ／ GEL off 1 ＝ CSS off ／ GEL on 2 ＝ CSS off ／ GEL blink 3 ＝ CSS on ／ GEL off 4 ＝ CSS on ／ GEL on 5 ＝ CSS on ／ GEL blink 6 ＝ CSS blink ／ GEL off 7 ＝ CSS blink ／ GEL on 8 ＝ CSS blink ／ GEL blink

F5 DF - Reset Nonvolatile Cfg Variables to Default

本コマンドは、すべての不揮発性 IPMI 設定をデフォルト値に強制的に設定します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**DF** コマンド指定子
	5:8	43 4C 52 AA ＝ ’CLR’0xaa：セキュリティコード
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 E0 - Reset ConfigSpace variables to default

本コマンドは、すべての設定スペース変数をデフォルトに強制的に設定します。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**E0** コマンド指定子
	5:8	43 4C 52 AA ＝ ’CLR’0xaa：セキュリティコード
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

F5 F8 - Delete User ID

システムでは最大 16 人のユーザーがサポートされます。本コマンドは、iRMC S2 ユーザーを個別に削除することができます。

重要！
すべての iRMC S2 ユーザーを削除するとシステムを管理することができなくなります。

要求データ	-	**B8** NetFnlLUN：OEM ／グループ
	-	**F5** Cmd：コマンドグループ BMC
	1:3	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト
	4	**F8** コマンド指定子
	5:8	ユーザー ID（1 ～ 16）
応答データ	-	**BC**
	-	**F5**
	1	完了コード
	2:4	**80 28 00** IANA-Enterprise-Number FTS、LSB ファースト

関連マニュアル一覧

ServerView Suite DVD 2 内には、次のマニュアルが格納されています。

➢ これらのマニュアルは、http://manuals.ts.fujitsu.com からもダウンロードできます。

[1] **ServerView Suite**
Basic Concepts

[2] **PRIMERGY Glossary**

[3] **PRIMERGY Abbriviations**

[4] **Secure PRIMERGY Server Management**
Enterprise Security
PRIMERGY server management for secure,
highly available platforms
White Paper

[5] **PRIMERGY ServerView Suite**
Installation Manager
User Guide

[6] **PRIMERGY ServerView Suite**
Deployment Manager
User Guide

[7] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation under Windows
Installation Guide

[8] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation under Windows
Quick Installation Guide

[9] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation under Linux
Installation Guide

[10] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Installation under Linux
Quick Installation Guide

[11] **PRIMERGY ServerView Suite**
ServerView S2
ServerView Agents (Linux, VMware)
Quick Installation Guide

[12] **PRIMERGY ServerView Suite**
ServerView Operations Manager
Server Management
User Guide

[13] **PRIMERGY ServerView Suite**
ServerView Inventory Manager

User Guide

[14] **PRIMERGY ServerView Suite**
ServerView Archive Manager
User Guide

[15] **PRIMERGY ServerView Suite**
Asset Management
Command Line Interface
User Guide

[16] **PRIMERGY ServerView Suite**
ServerView RAID Manager
User Guide

[17] **PRIMERGY ServerView Suite**
ServerView Event Manager
User Guide

[18] **PRIMERGY ServerView Suite**
ServerView Threshold Manager
User Guide

[19] **PRIMERGY ServerView Suite**
ServerView Performance Manager
User Guide

[20] **PRIMERGY ServerView Suite**
ServerView Download Manager
ServerView
User Guide

[21] **PRIMERGY ServerView Suite**
ServerView Update Manager
User Guide

[22] **PRIMERGY ServerView Suite**
ServerView Update Manager Express
User Guide

[23] **PRIMERGY ServerView Suite**
PrimeUp
User Guide

[24] **PRIMERGY ServerView Suite**
Bootable Update CD
User Guide

[25] **PRIMERGY ServerView Suite**
ServerView Online Diagnostics
User Guide

[26] **PRIMERGY ServerView Suite**
Local Service Concept (LSC)
User Guide

[27] **PRIMERGY ServerView Suite**
PrimeCollect
User Guide

[28] **PRIMERGY ServerView Suite**
ServerView Virtual-IO Manager
User Guide

[29] **PRIMERGY ServerView Suite**
ServerView Virtual-IO Manager CLI
Command Line Interface

[30] **PRIMERGY ServerView Suite**
ServerView Integration
Overview

[31] **PRIMERGY ServerView Suite**
ServerView Integration in MOM
User Guide

[32] **PRIMERGY ServerView Suite**
ServerView Integration Pack for MS SCOM
User Guide

[33] **PRIMERGY ServerView Suite**
ServerView Integration Pack for MS SMS
User Guide

[34] **PRIMERGY ServerView Suite**
DeskView and ServerView Integration Pack for Microsoft SCCM
User Guide

[35] **PRIMERGY ServerView Suite**
ServerView Integration in HP OpenView NNM
User Guide

[36] **PRIMERGY ServerView Suite**
ServerView Integration in HP Operations Manager
User Guide

[37] **PRIMERGY ServerView Suite**
ServerView Integration Pack in Tivoli NetView
User Guide

[38] **PRIMERGY ServerView Suite**
ServerView Integration Pack in Tivoli TEC
User Guide

[39] **PRIMERGY ServerView Suite**
ServerView Integration in DeskView
User Guide

[40] **PRIMERGY ServerView Suite**
ServerView Remote Management Frontend
User guide

[41] **PRIMERGY ServerView Suite**
iRMC - integrated Remote Management Controller
User Guide

[42] **PRIMERGY ServerView Suite**
iRMC S2 - integrated Remote Management Controller
User Guide

[43] **PRIMERGY ServerView Suite**
Provision of ServerView Software on the Internet
Description

[44] **PRIMERGY BX300 Blade Server Systems**
Operating Manual

[45] **PRIMERGY BX600 Blade Server Systems**
Operating Manual

[46] **PRIMERGY BX600 Blade Server Systems**
ServerView Management Blade S3
User Interface Description
User Guide

[47] **PRIMERGY BX900 Blade Server Systems**
Operating Manual

[48] **PRIMERGY BX900 Blade Server**
Systems ServerView Management Blade S1
User Interface Description
User Guide

[49] **PRIMERGY Blade Server System**
LAN Switch Blade
User Interface Description
User Guide

[50] **BIOS-Setup**
Description

[51] **PRIMEPOWER ServerView Suite**
System Administration within a Domain
User Guide

[52] **FibreCAT CX**
Monitoring FibreCAT SX systems with ServerView Operations Manager
Welcome Guide

[53] **FibreCAT SX**
Monitoring FibreCAT SX systems with ServerView Operations Manager
Welcome Guide

[54] **StorMan**
Provisioning and managing virtualized storage resources
Administrator and User Guide

[55] **APC network management card**
User’s Guide

[56] **VMware**
VMware ESX Server
Installation Guide

[57] **VMware**
VMware ESX Server
Administration Guide

索引

A

B

K

L

Q